互联 Cisco 网络设备第 2 部分 (ICND2 v1.0)

© 2008 Cisco Systems, Inc. 保留所有权利。

课程简介

© 2008 Cisco Systems, Inc. 保留所有权利。

学员的技能和知识

- 与*互联 Cisco 网络设备第 1 部分*内容等同的知识和技能
  - 能解释 OSI 模型，并能识别网络的组成部分
  - 能说明以太网问题的交换 LAN 技术解决方案
  - 能说明路由如何扩展网络
  - 能理解 TCP/IP 的主机到主机数据包传输过程
  - 能说明 WAN 的功能
  - 能使用 Cisco 命令行界面实现小型网络的安装、配置和故障排除
  - 能管理路由器和交换机的启动和配置

© 2008 Cisco Systems, Inc. 保留所有权利。

课程目标

“中型网络的建立、操作和故障排除，包括连接到 WAN 和实施网络安全”

互联 Cisco 网络设备第 2 部分

© 2008 Cisco Systems, Inc. 保留所有权利。

课程总体管理

课堂相关管理

- 签到簿
- 长度和时间
- 休息室和午餐室的位置
- 着装

设施相关管理

- 课程资料
- 所在地点紧急事件程序
- 休息室
- 电话和传真

© 2008 Cisco Systems, Inc. 保留所有权利。

课程流程

	第 1 天	第 2 天	第 3 天	第 4 天	第 5 天
上午	课程简介 小型网络实施	中型交换网络结构（续）	中型路由网络结构（续）	EIGRP 实施（续）	地址空间管理（续）
			单区域 OSPF 实施	访问控制列表	LAN 延伸到 WAN
	午餐				
下午	中型交换网络结构	中型路由网络结构	单区域 OSPF 实施（续）	访问控制列表（续）	LAN 延伸到 WAN（续）
			EIGRP 实施	地址空间管理	

© 2008 Cisco Systems, Inc. 保留所有权利。

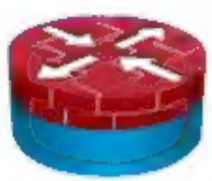
Cisco 图标和符号

路由器

集线器

网云

工作组
交换机


带防火墙
的路由器

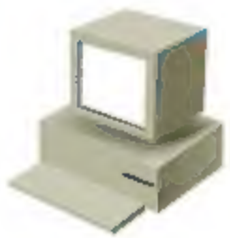
帧交换机

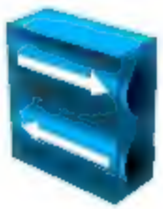
终端
服务器

IP 电话

Cisco ASA 5500

多层
交换机


个人电脑


VPN
集中器

带路由 / 交换
处理器的多层
交换机

服务器

PIX
防火墙

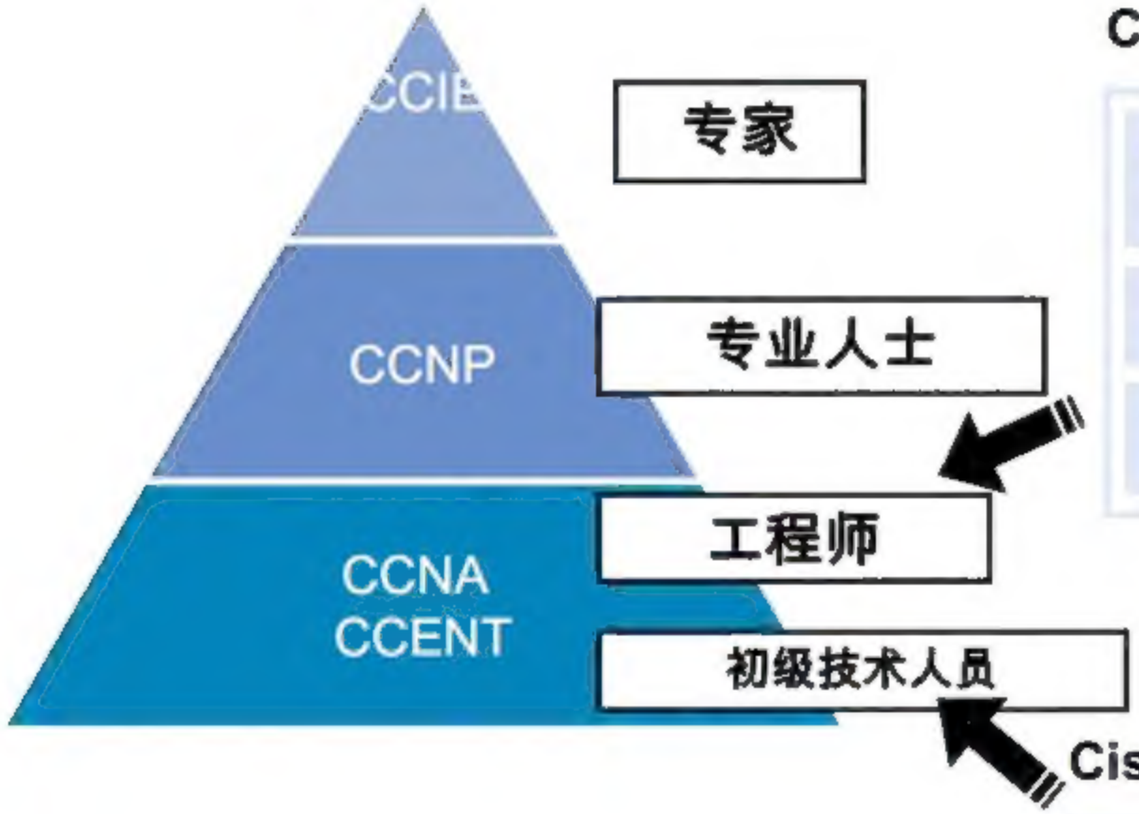
© 2008 Cisco Systems, Inc. 保留所有权利。

Cisco 职业认证

© 2008 Cisco Systems, Inc. 保留所有权利。

Cisco 职业认证

延伸您的专业选择、拓展您的职业道路



Cisco Certified Network Associate

Cisco 学习合作伙伴
推荐的培训

互联 Cisco 网络设备第 1 部分

互联 Cisco 网络设备第 2 部分

Cisco Certified Entry Network Technician

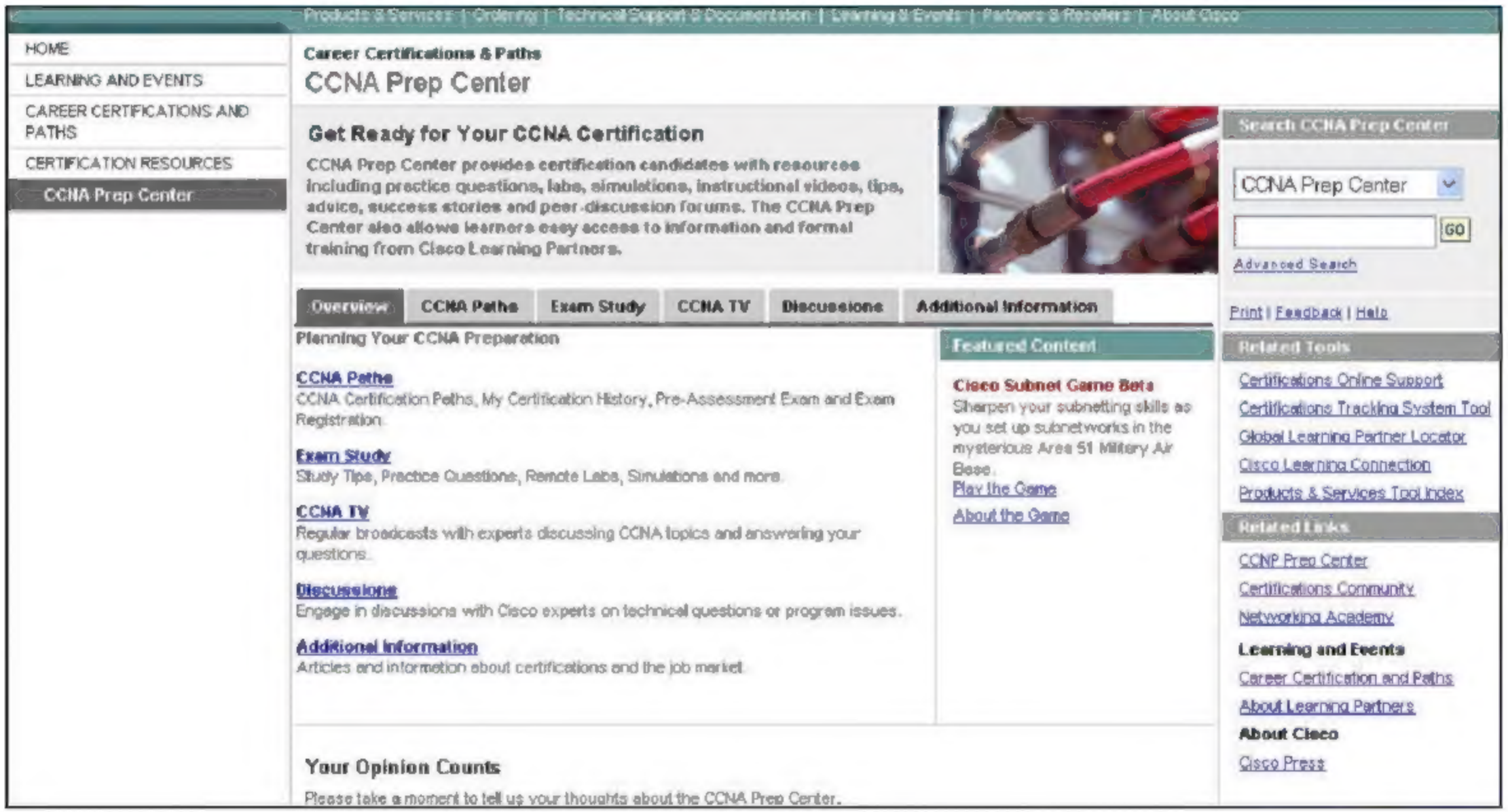
Cisco 学习合作伙伴
推荐的培训

互联 Cisco 网络设备第 1 部分

www.cisco.com/go/certifications

© 2008 Cisco Systems, Inc. 保留所有权利。

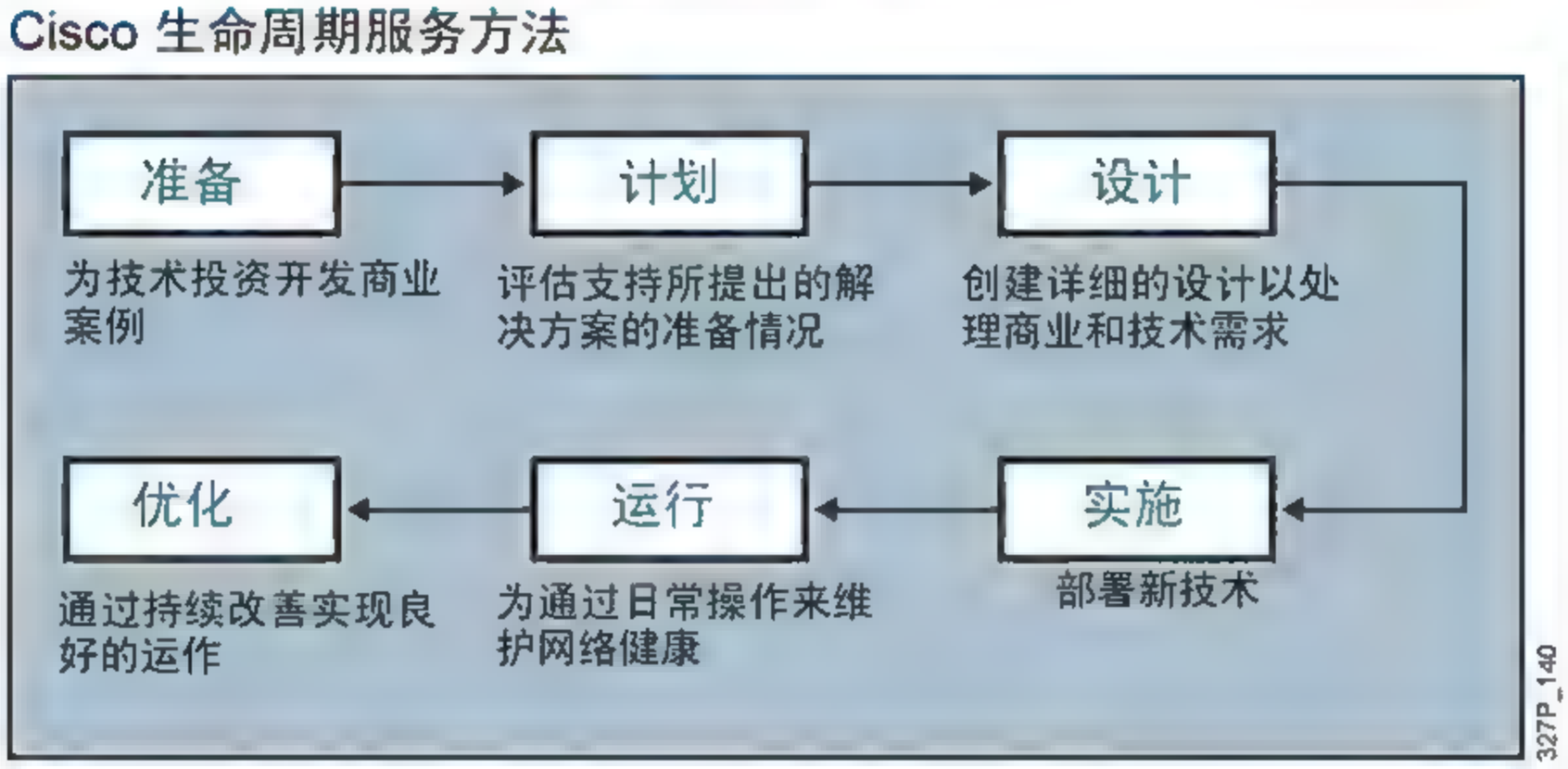
CCNA 备考中心



www.cisco.com/go/prepcenter

© 2008 Cisco Systems, Inc. 保留所有权利。

什么是生命周期服务框架？

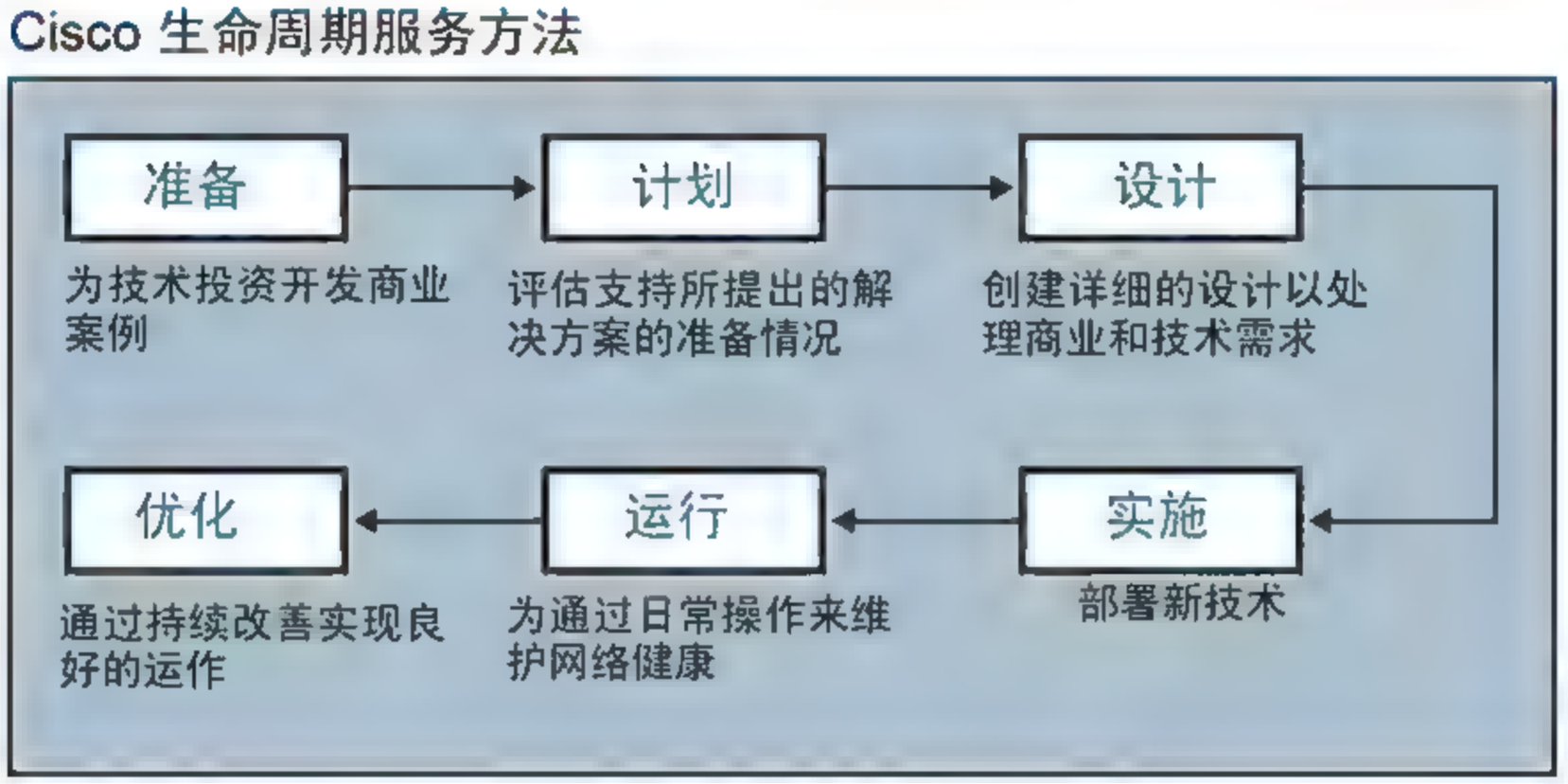


- Cisco 生命周期服务框架定义了在整个网络生命周期内成功部署、运行和优化 Cisco 技术所必须采取的措施。
- 网络生命周期分为六个阶段：准备、计划、设计、实施、运行以及优化。
- 每个阶段都有一组服务组件，包括用于确保优质服务的活动和交付成果。服务项目完成之后将执行网络服务。

CCNA 学员：重点关注“实施”和“运行”

阶段	生命周期服务方法的优点
准备	通过商务案例制定稳健的财务决策，为技术革新建立财务评价。
计划	评估现有环境以确定其是否能充分而安全地支持所提议的系统。
设计	设计出满足业务需求和技术需求的解决方案。
实施	在不中断现有网络或不形成漏洞的前提下整合新解决方案。
运行	通过日常操作来维护网络正常运行。
优化	通过调整网络的体系结构、运行和性能实现良好的运营，从而满足不断变化的业务需求，并将自身定位于重新进入生命周期的准备阶段。

网络生命周期服务方法：为什么该方法现在很重要？



- 在过去，设计、实施和运行阶段的点汇入方法足以部署和支持网络。
- 如今，网络复杂性和技术融合使拥有可随时适应不断变化之业务状况的网络生命周期方法显得更加重要。协调而持续的生命周期服务活动序列能够使初步实施和运行获得成功，还可进一步优化性能。
- Cisco 生命周期服务方法有助于满足这些更复杂的新要求。

学员简介

- 您的姓名
- 您的公司
- 职务
- 技能和知识
- 简历
- 目标

复习实验简介

小型网络的实施

Cisco IOS 用户界面功能

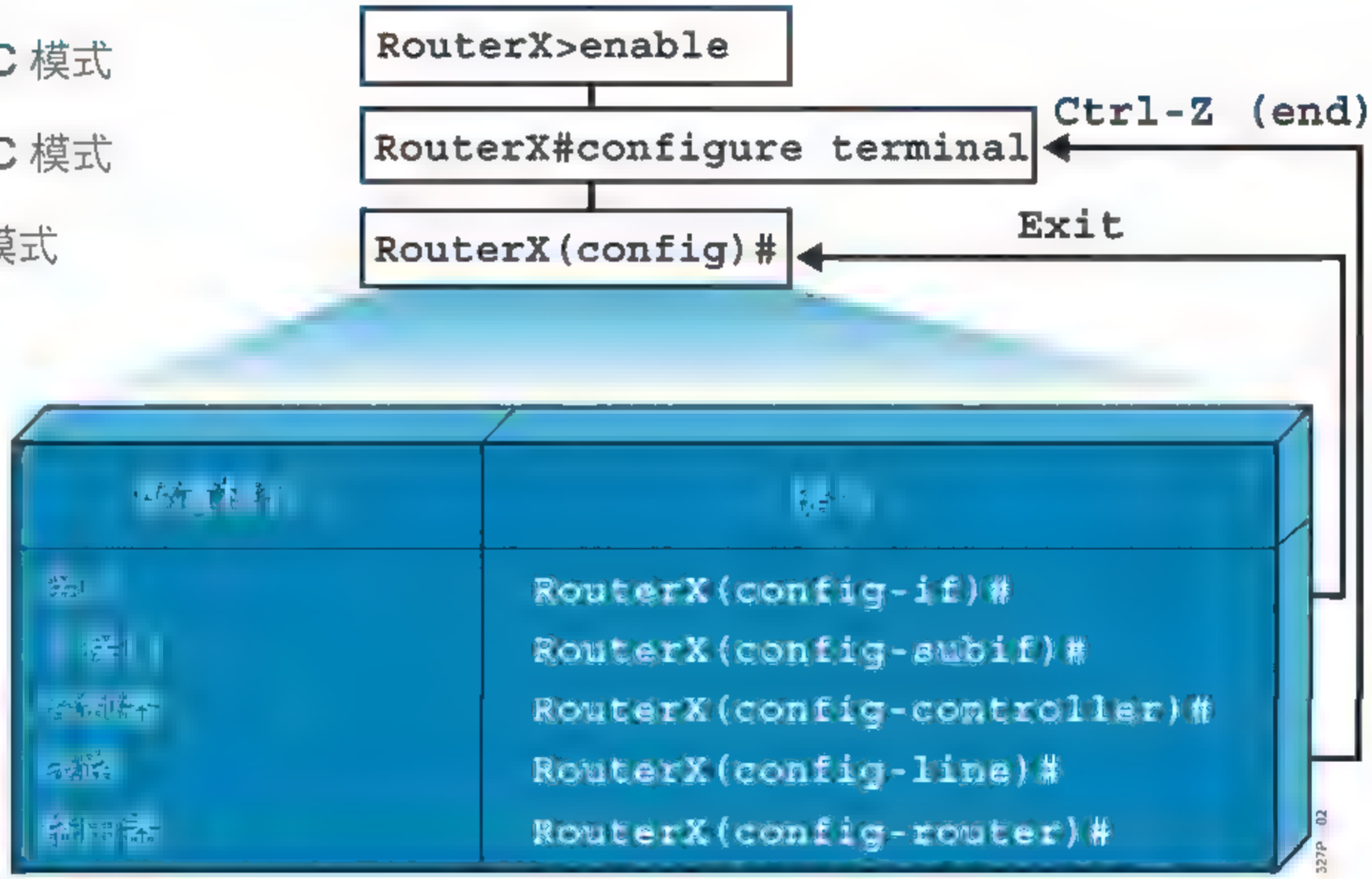
- CLI 用于输入命令。
- 路由器或交换机的操作会有所不同，但都使用同样的 CLI。
- 按 **Enter** 键可让设备解析并执行命令。
- CLI 在其配置模式结构中采用分级命令。
- 用户可以在控制台配置模式中键入或粘贴输入。
- 配置模式都具有独特的提示符。
- 两种主要的 EXEC 模式是用户模式和特权模式。
- 不会自动保存更改。

Cisco IOS 配置模式概述

用户 EXEC 模式

特权 EXEC 模式

全局配置模式



© 2008 Cisco Systems, Inc. 保留所有权利。

Cisco IOS CLI 的帮助工具

[illegible]

提供命令列表以及
特定命令的相关参数

[illegible]

确认与错误输入的任何
交换机命令相关的问题，
以便进行修改和纠正

命令历史记录缓冲区

允许重新调用较长或较复杂的
命令或输入项以供重新输入、
检查或纠错

© 2008 Cisco Systems, Inc. 保留所有权利。

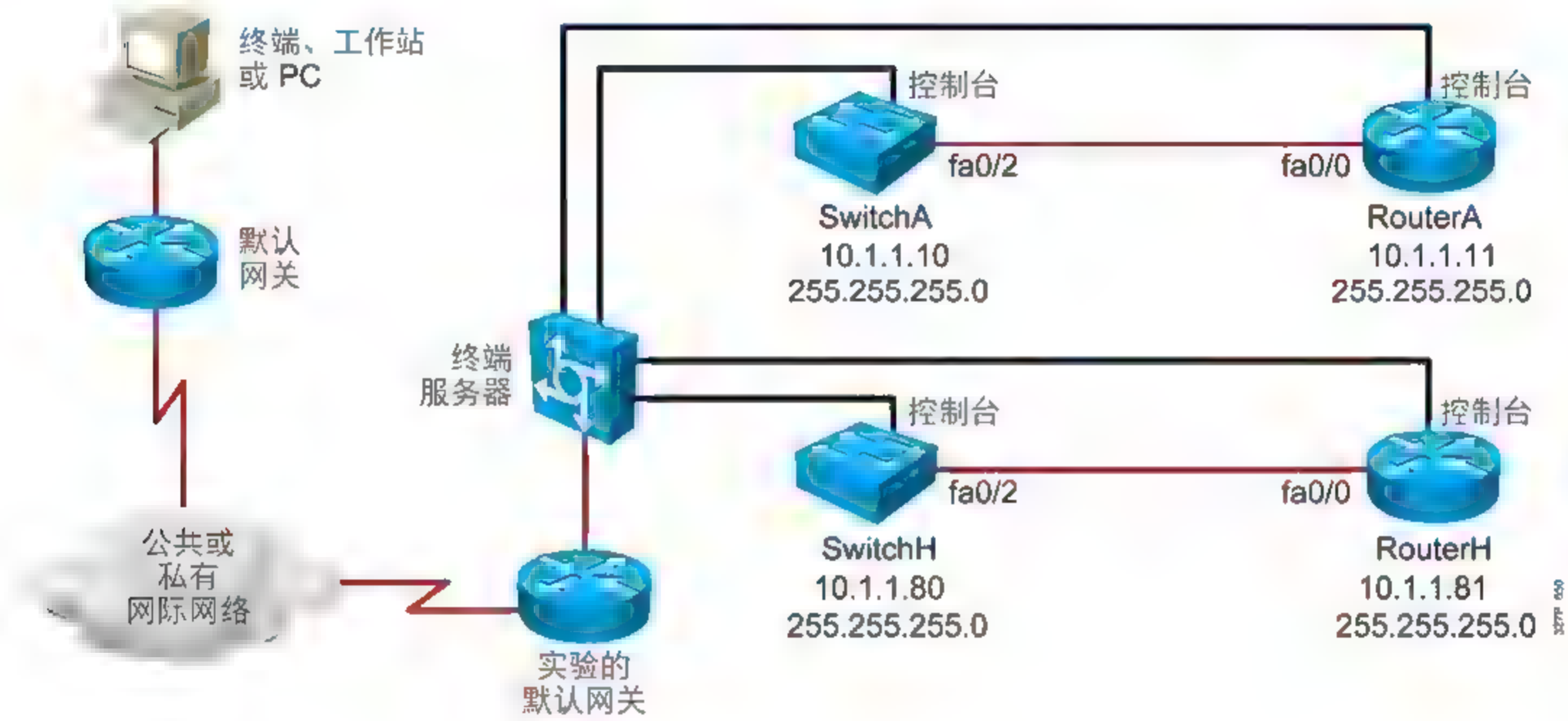
命令复习讨论

banner motd	configure terminal	copy running-config startup-config	enable	enable secret password
erase startup-configuration	hostname *name*	interface *interface*	ip address *address mask*	ip default-gateway *address*
line console 0	line vty 0 4	login	password *password*	reload
show cdp neighbors	show interfaces	show port-security [interface address]	show running-configuration	show startup-configuration
shutdown/no shutdown	switchport mode access	switchport port-security	switchport port-security mac-address *mac*	switchport port-security maximum *value*

327P 631

- 命令能够完成什么操作？
- 命令要从何种配置模式中执行？

接入远程实验室



使用此单元复习来完成引导性实验，该实验将成为所有后续实验练习的基础。

总结

- 基本的路由器或交换机配置包括：提供用于识别身份的主机名、提供用于安全保护口令的规则，以及分配用于连接的 IP 地址。
- 使用 CLI 输入命令。
- 使用 **configure terminal** 命令进入全局配置模式。要退出全局配置模式，可使用命令 **end** 或按 **Ctrl-Z**。
- CLI 提供对上下文敏感的帮助、控制台错误消息和命令历史记录缓冲区。

单元总结

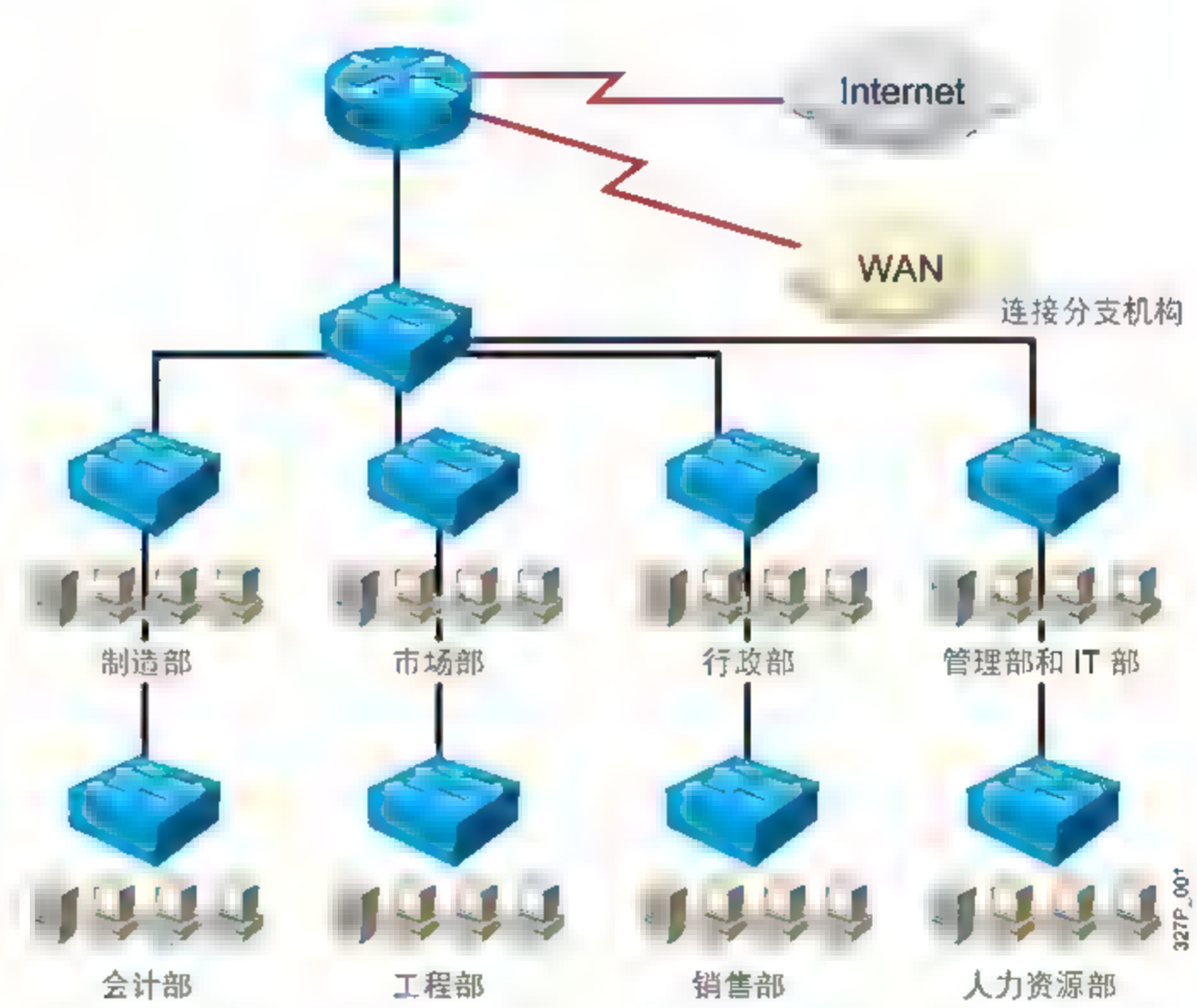
- Cisco IOS CLI 为配置路由器和交换机提供了分层配置模式。
- 您将使用此界面作为实施满足小型网络设计要求的基本交换网络和路由网络的工具。

实施 VLAN 和中继

中型交换网络结构

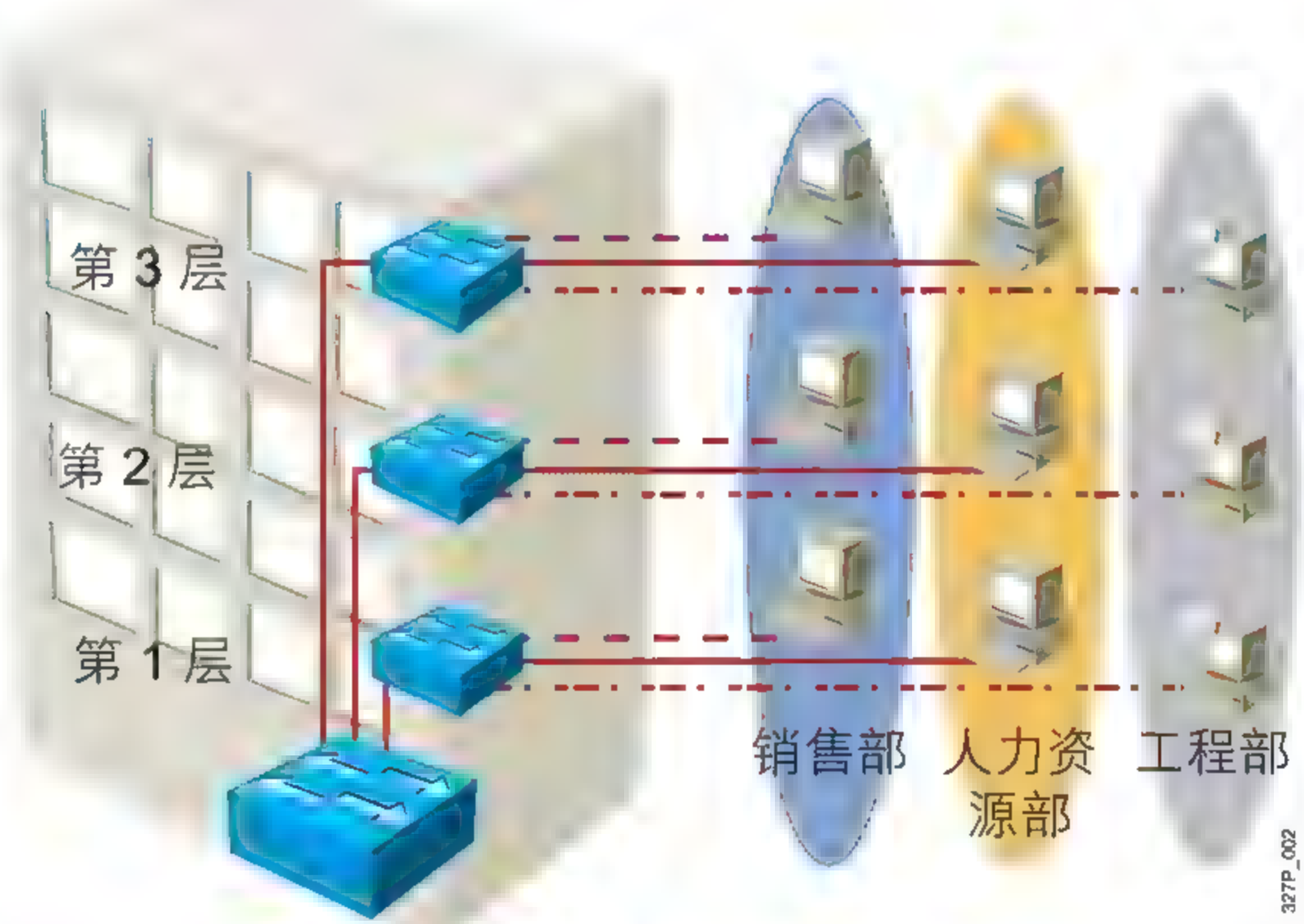
设计欠佳的网络中存在的问题

- 极大的故障域
- 较大的广播域
- 大量的未知 MAC 单播流量
- 极大的组播流量
- 管理和支持上的挑
- 可能存在安全漏洞



VLAN 概述

- 分段
- 灵活性
- 安全性

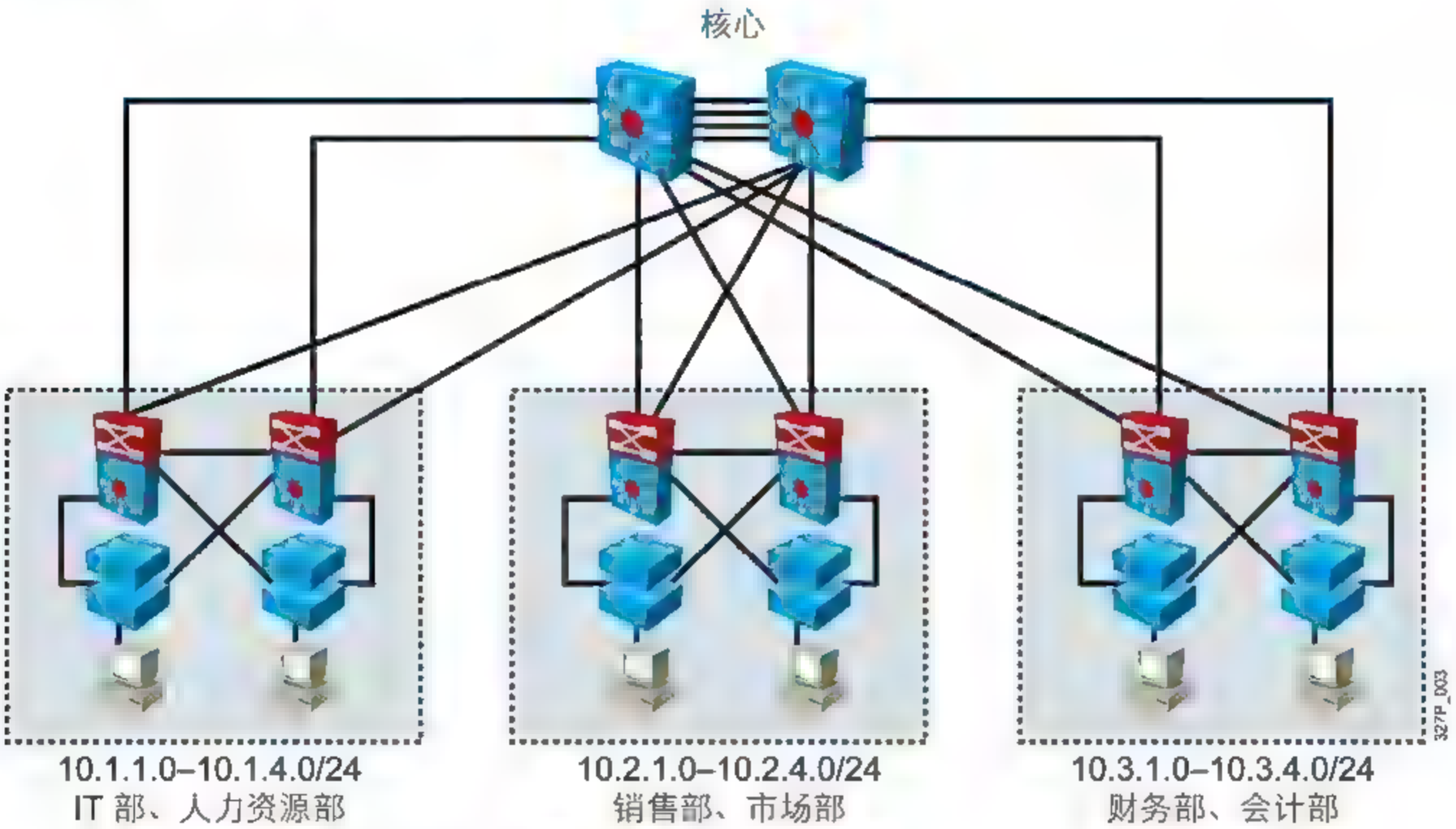


VLAN = 广播域 = 逻辑网络（子网）

为组织设计 VLAN

- VLAN 的设计必须考虑如何实施分层网络编址方案。
- 分层编址的优点包括：
  - 易于管理和故障排除
  - 错误数量最小化
  - 减少路由表的条目数

应用 IP 地址空间的指导原则

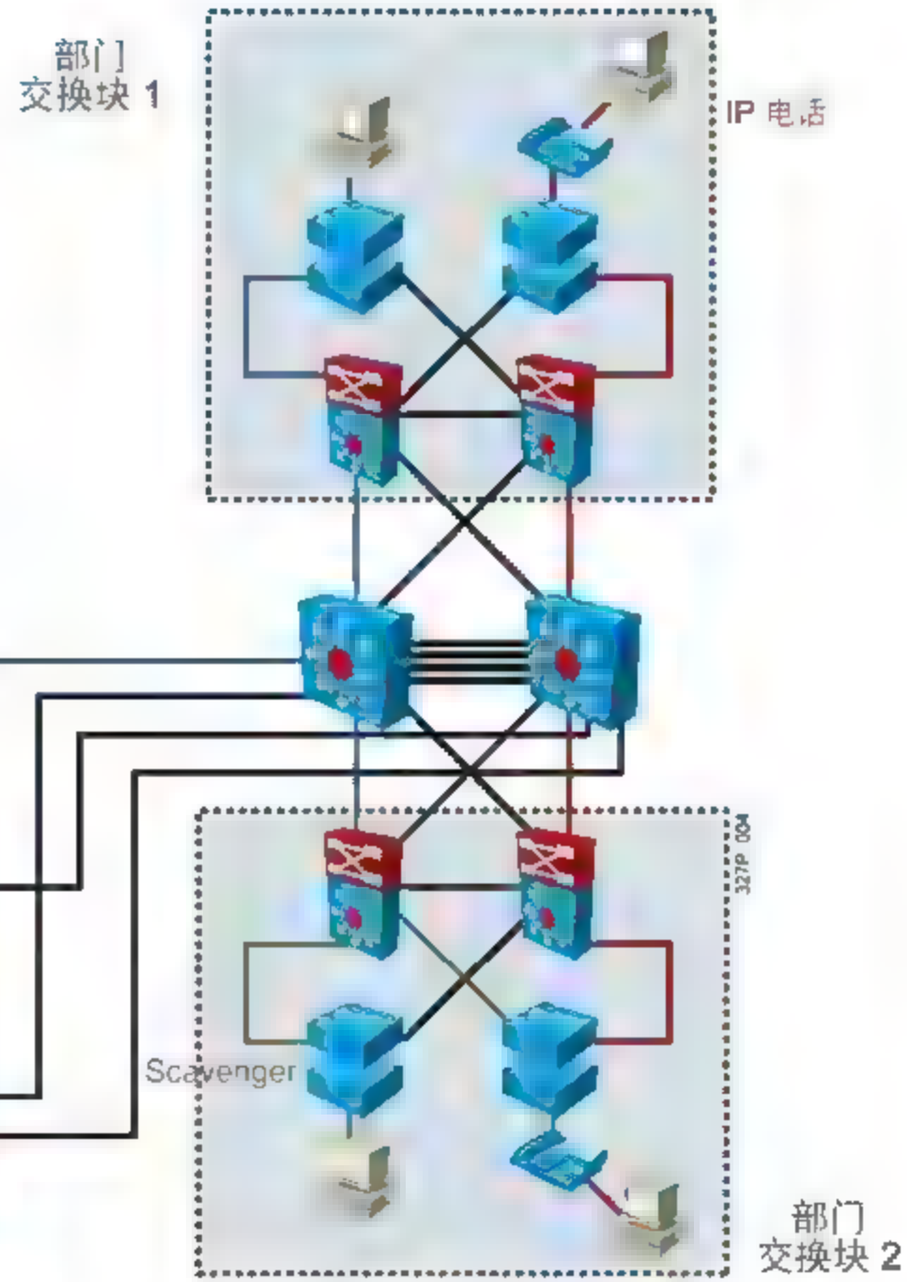


- 为每个 VLAN 分配一个 IP 子网。
- 在连续的地址块内分配 IP 地址空间。

网络流量类型

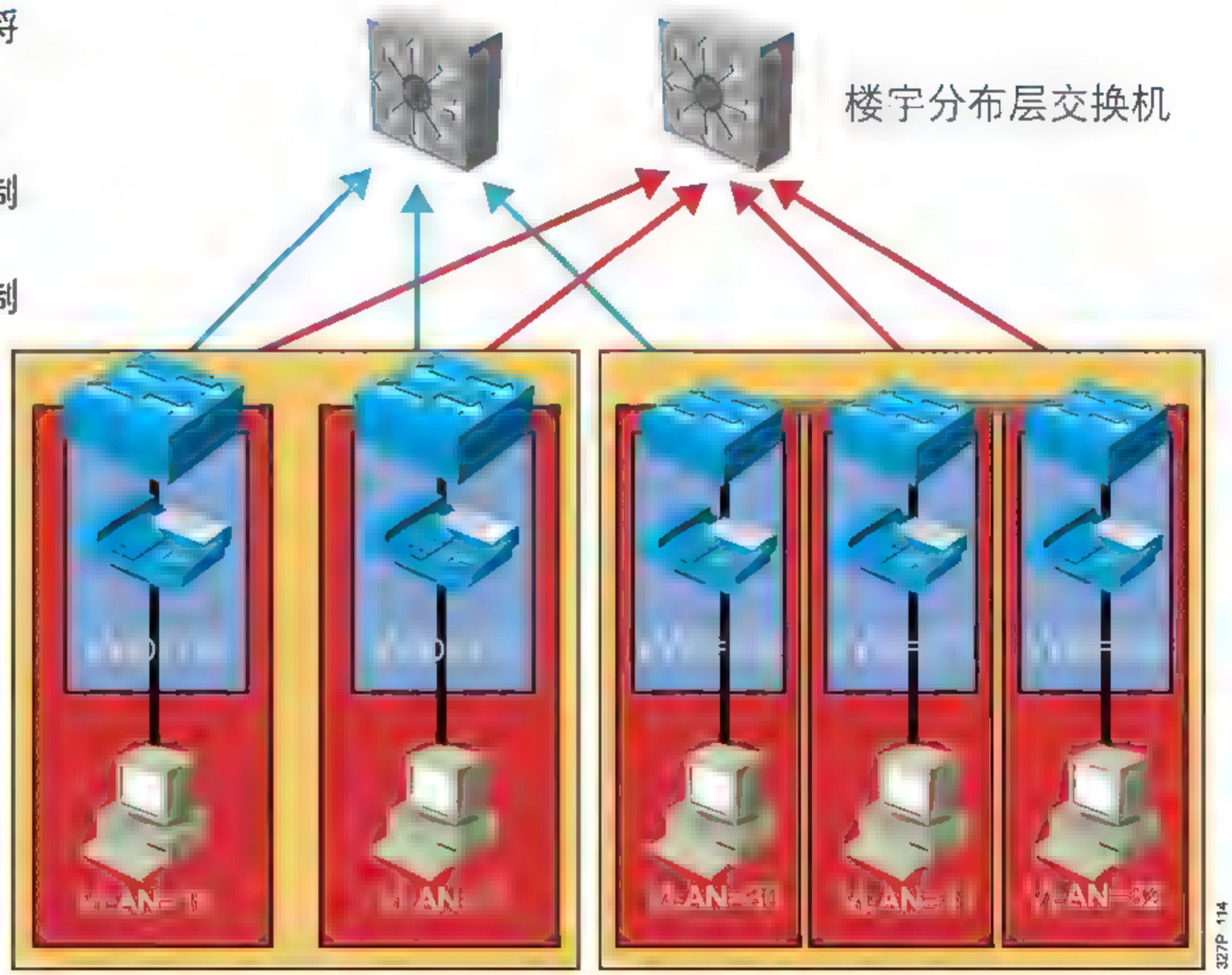
设计 VLAN 时需要考虑的流量类型：

- 网络管理
- IP 电话
- IP 组播
- 普通数据
- Scavenger 类型

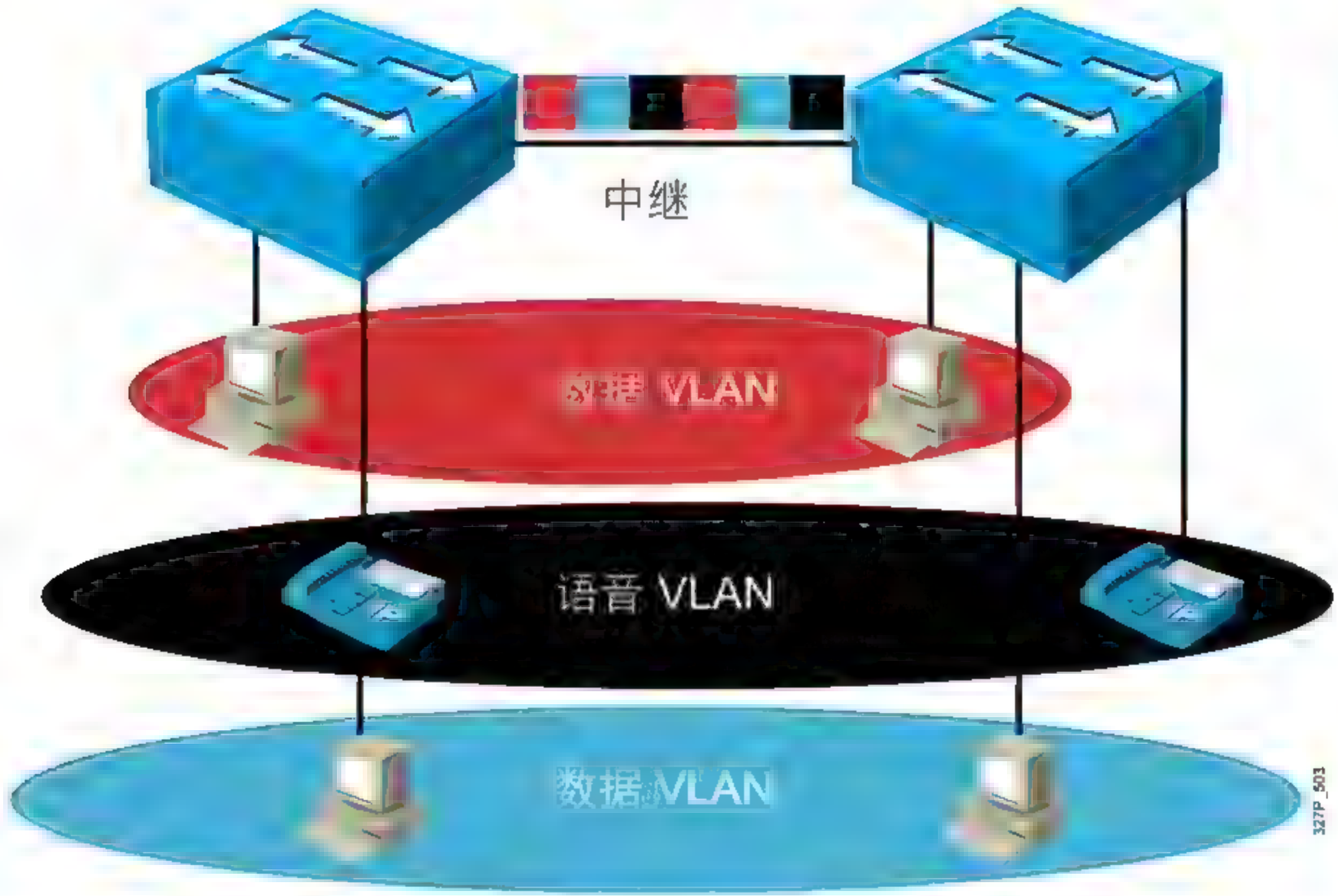


语音 VLAN 的优点

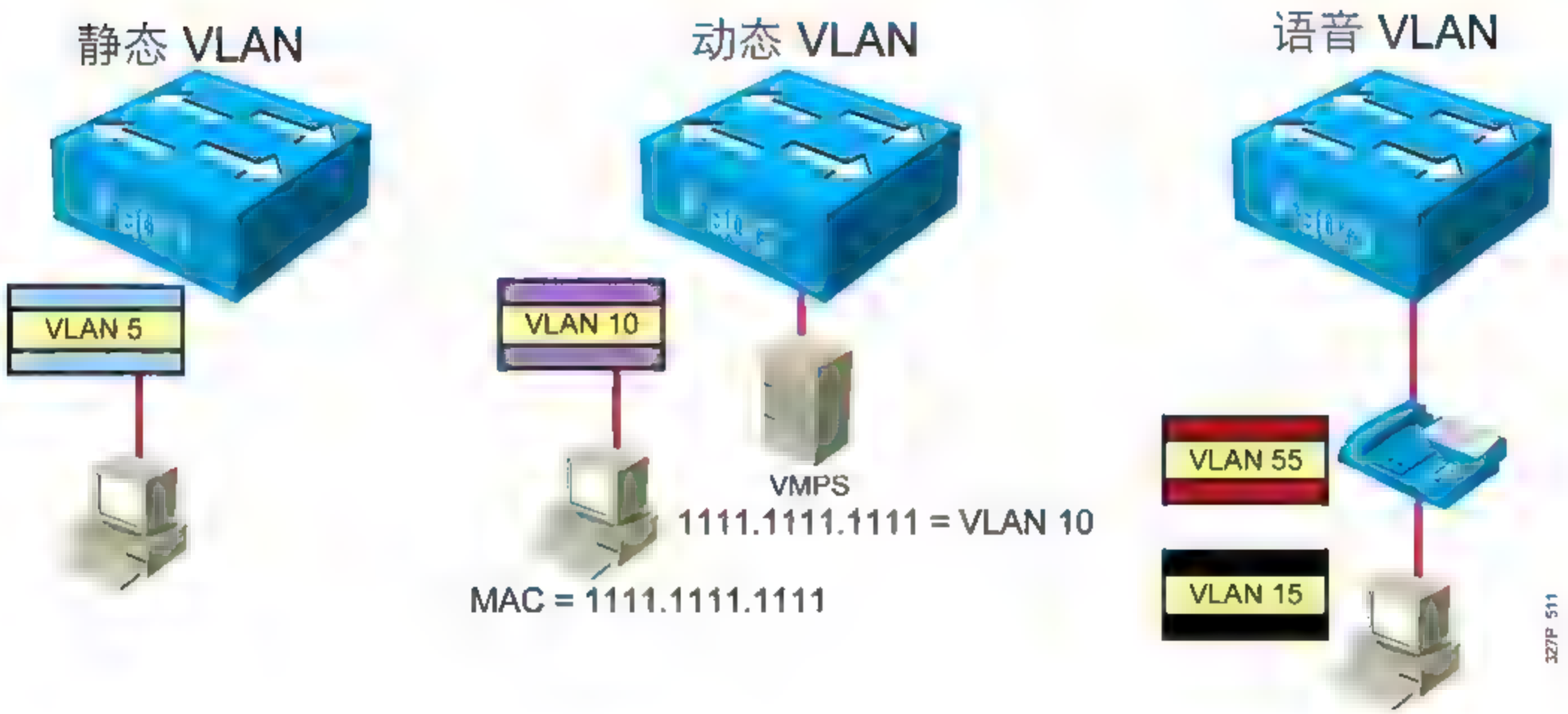
- 在独立的逻辑网络中将电话分段
- 提供网络分段和控制
- 允许管理员创建和强制实施 QoS
- 可让管理员添加和强制实施安全策略



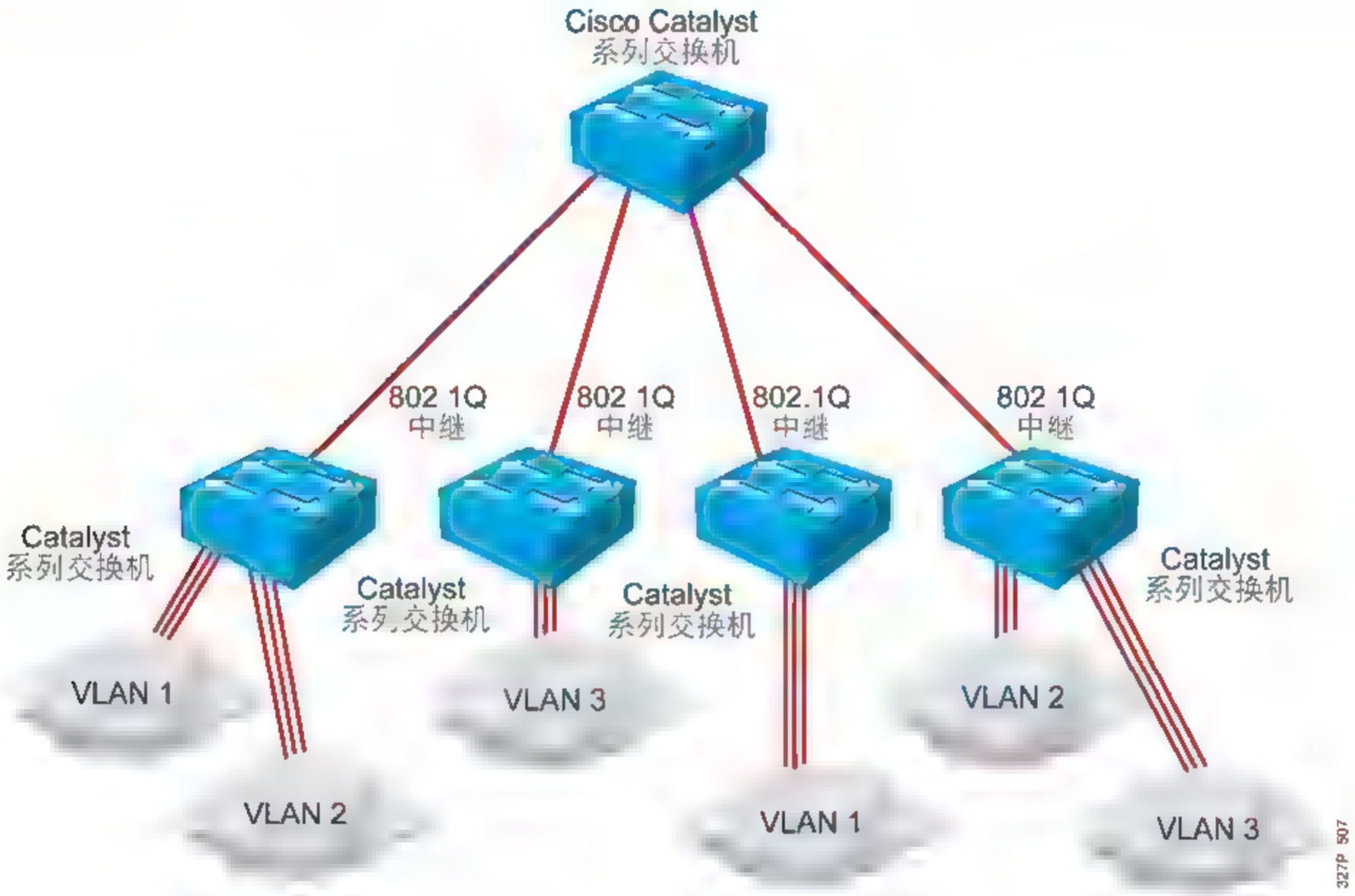
运行 VLAN



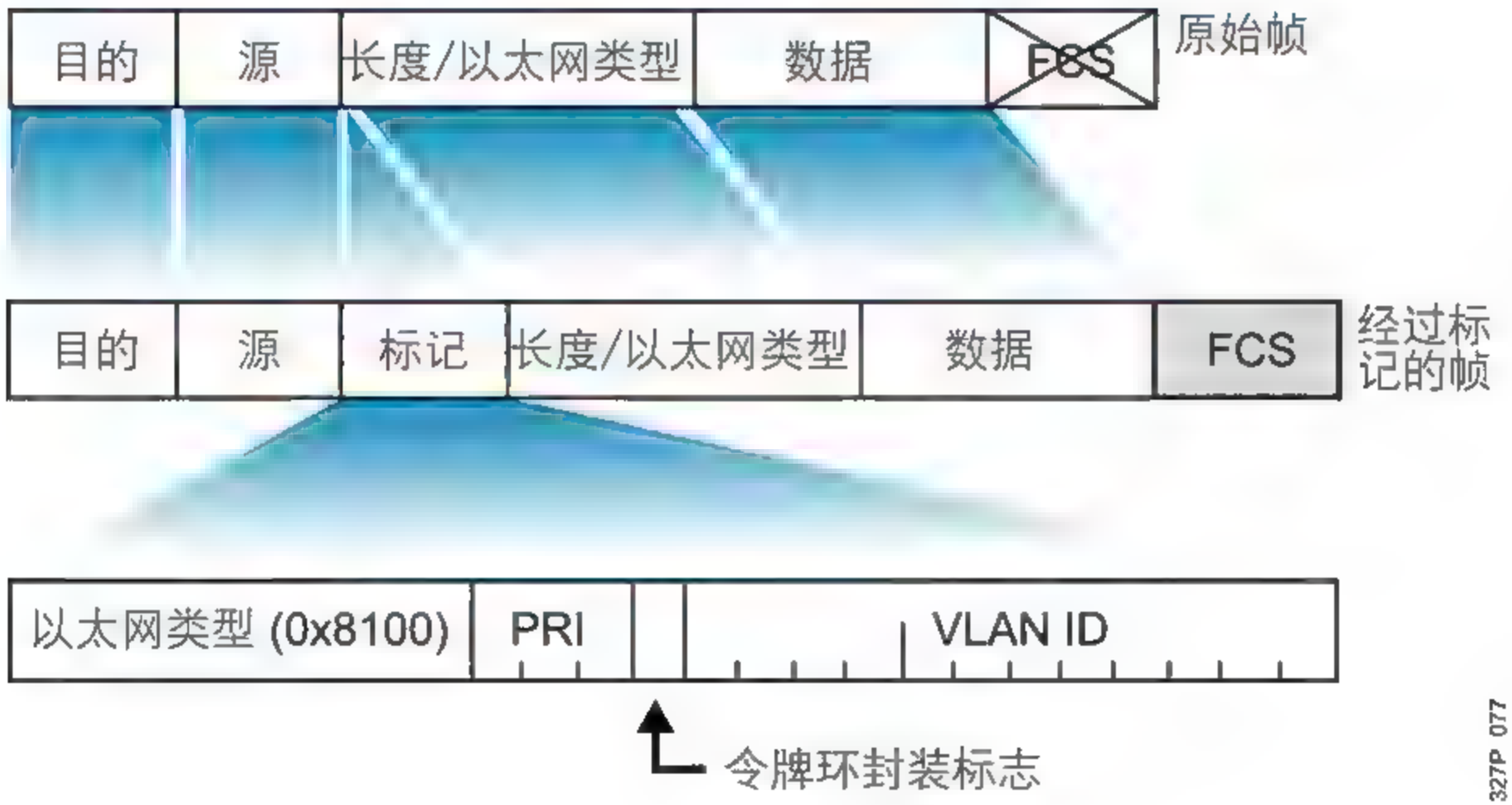
VLAN 成员资格模式


静态 VLAN
VLAN 5
动态 VLAN
VLAN 10
VMPS
1111.1111.1111 = VLAN 10
MAC = 1111.1111.1111
语音 VLAN
VLAN 55
VLAN 15
327F 511

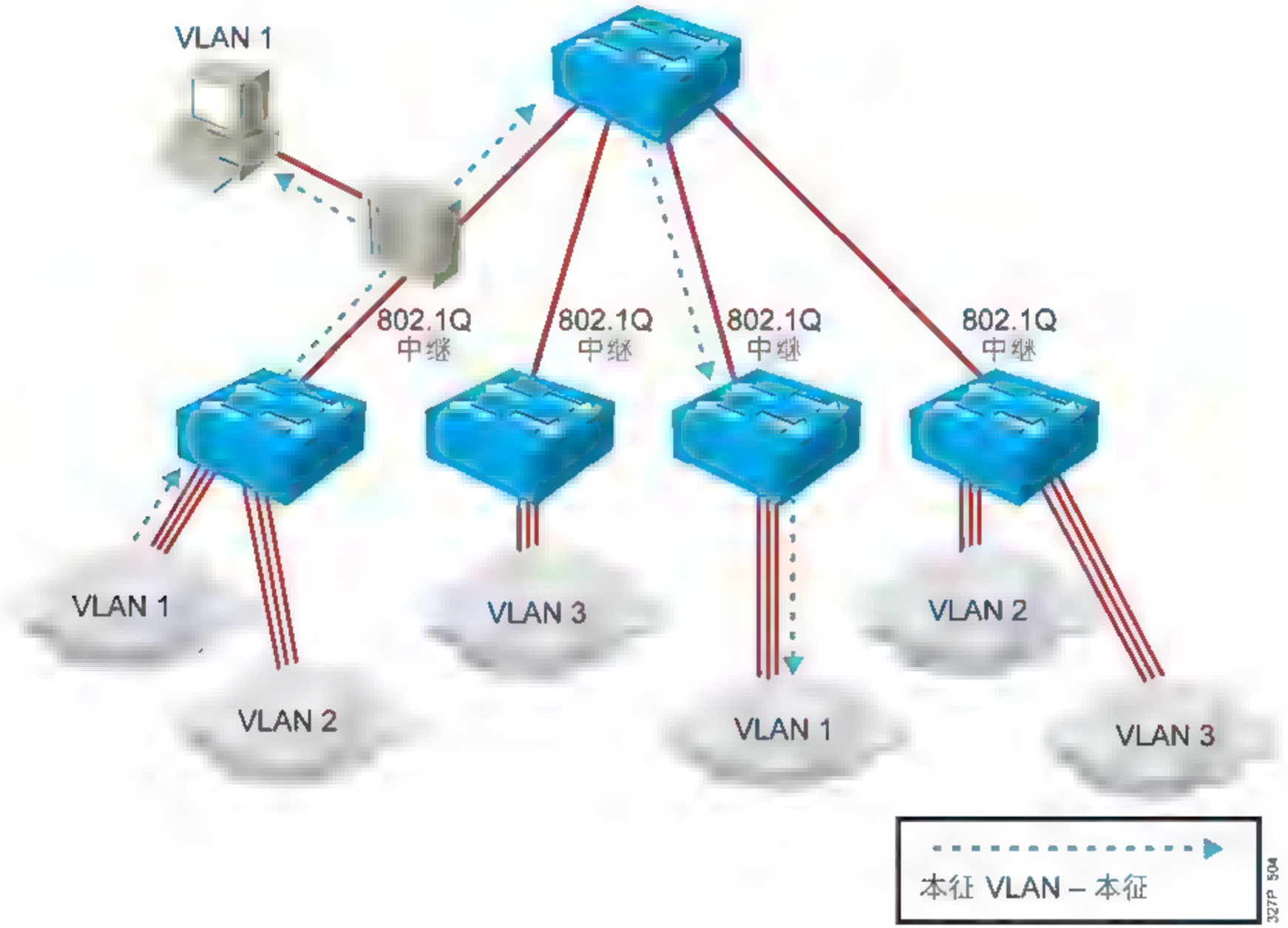
802.1Q 中继


Cisco Catalyst
系列交换机
802 1Q
中继
802 1Q
中继
802.1Q
中继
802 1Q
中继
Catalyst
系列交换机
Catalyst
系列交换机
Catalyst
系列交换机
Catalyst
系列交换机
VLAN 1
VLAN 2
VLAN 3
VLAN 1
VLAN 2
VLAN 3
327P 507

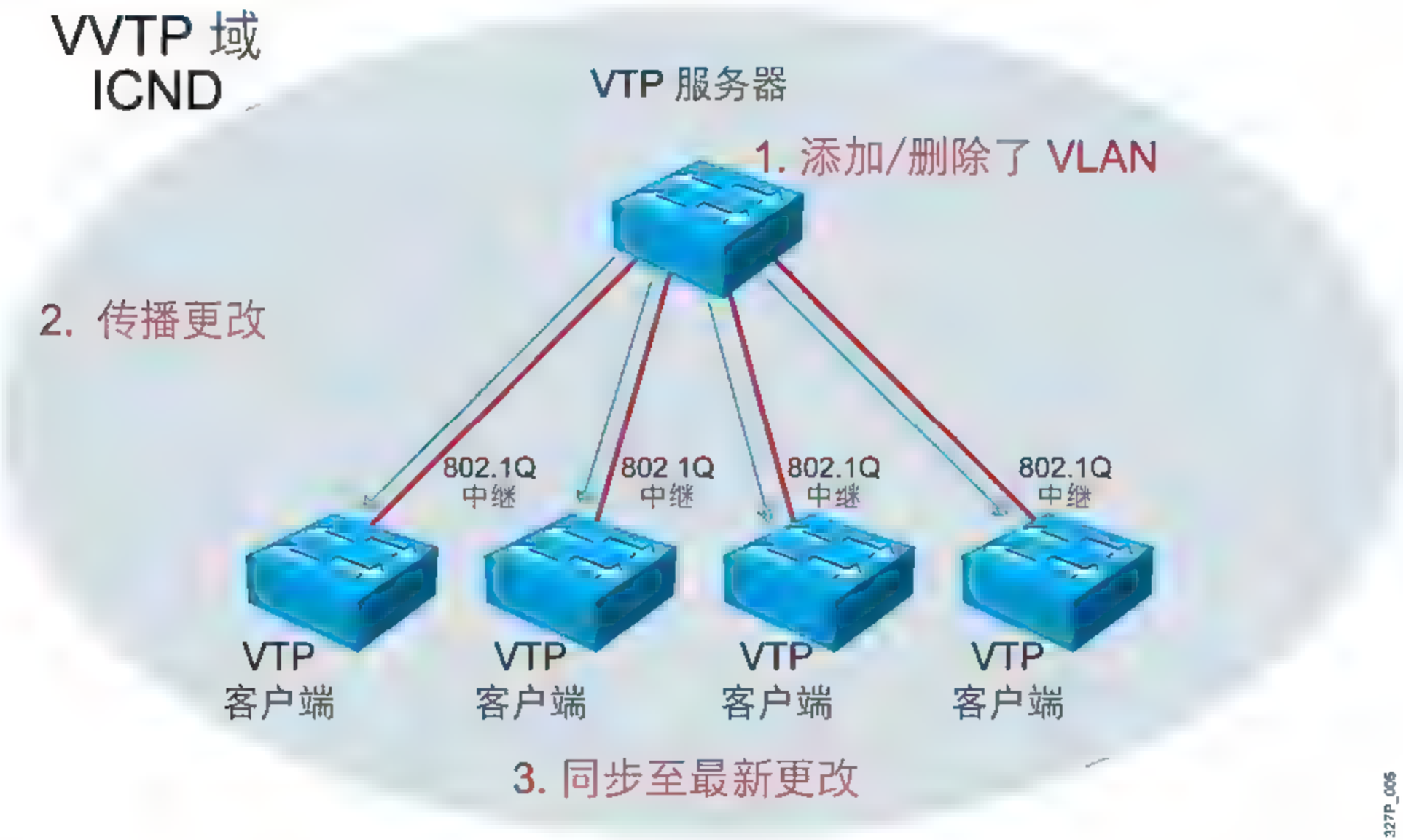
802.1Q 帧


目的
源
长度/以太网类型
数据
FCS
原始帧
目的
源
标记
长度/以太网类型
数据
FCS
经过标记的帧
以太网类型 (0x8100)
PRI
VLAN ID
令牌环封装标志
327P 077

了解本征 VLAN


VLAN 1
802.1Q
中继
802.1Q
中继
802.1Q
中继
802.1Q
中继
VLAN 1
VLAN 2
VLAN 3
VLAN 1
VLAN 2
VLAN 3
本征 VLAN – 本征
327P 504

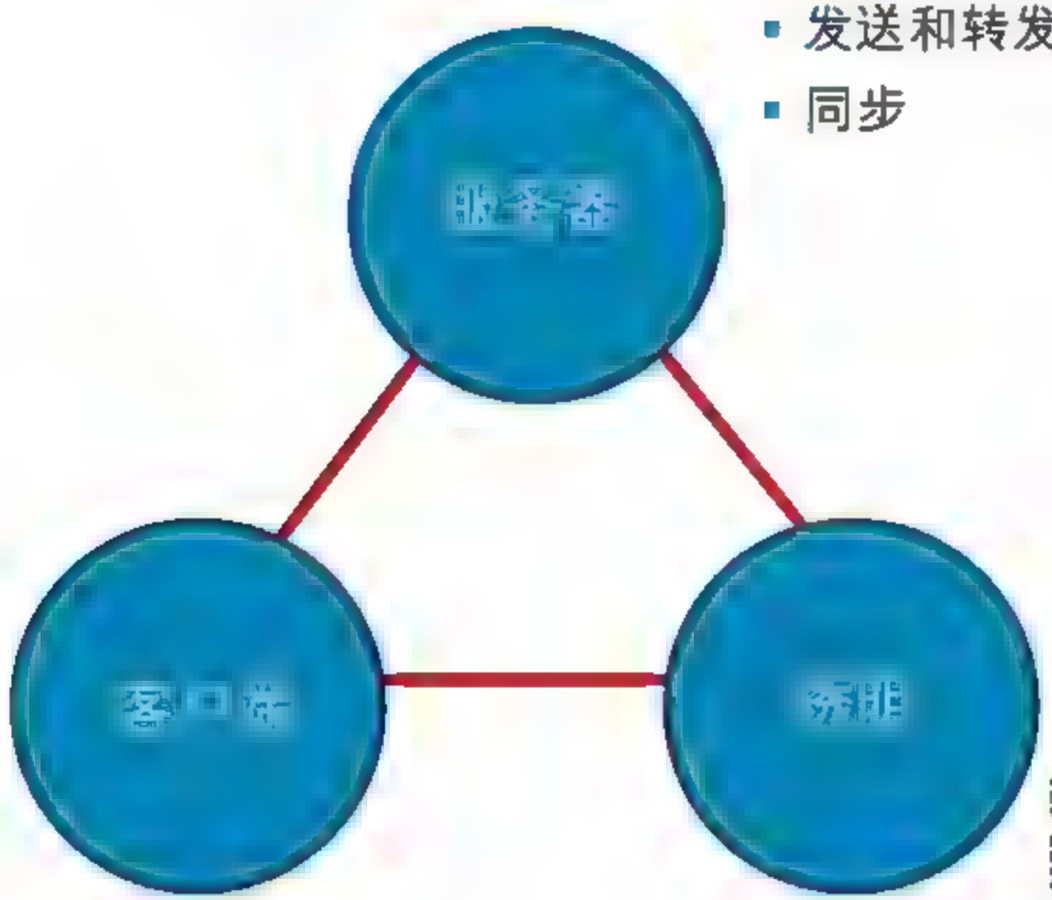
VTP 的功能


VVTP 域
ICND
VTP 服务器
1. 添加/删除了 VLAN
2. 传播更改
802.1Q
中继
802 1Q
中继
802.1Q
中继
802.1Q
中继
VTP
客户端
VTP
客户端
VTP
客户端
VTP
客户端
3. 同步至最新更改

VTP 模式

- 创建 VLAN
- 修改 VLAN
- 删除 VLAN
- 发送和转发通告
- 同步

- 无法创建、修改或删除 VLAN
- 发送和转发通告
- 同步



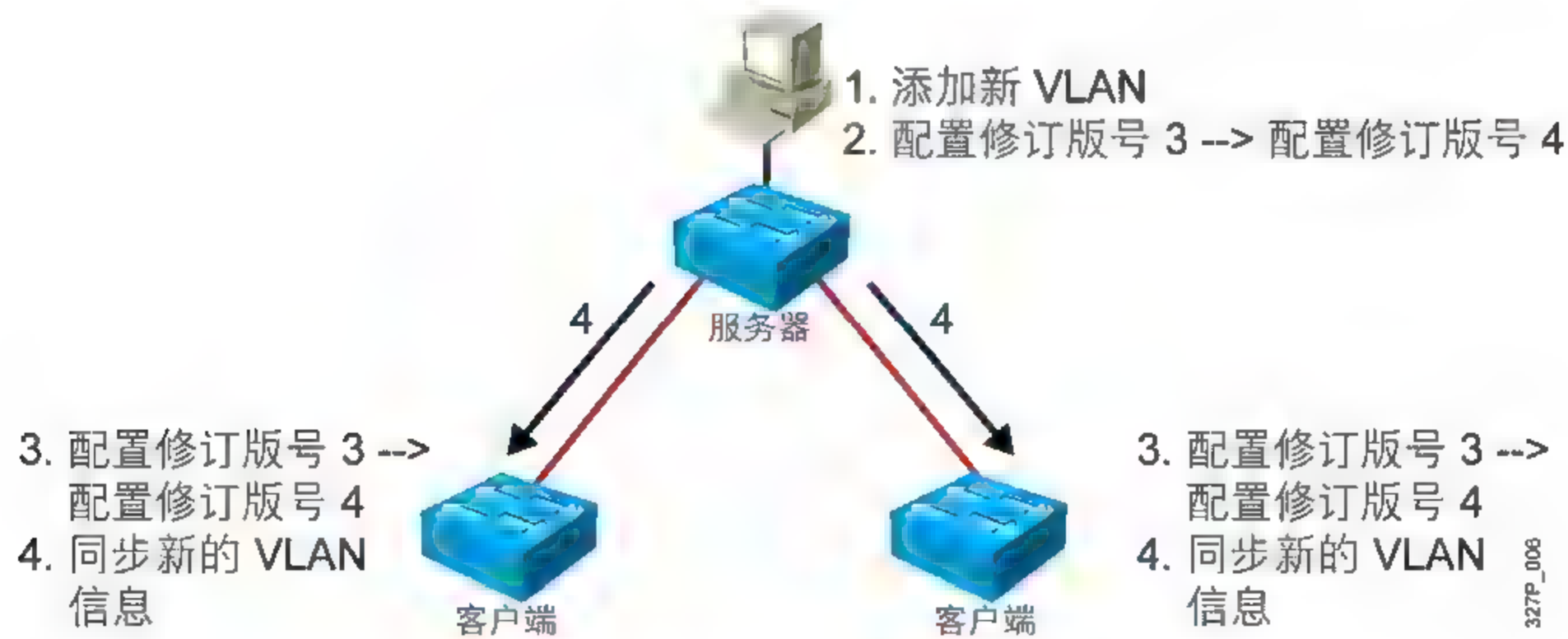
- 仅创建本地 VLAN
- 仅修改本地 VLAN
- 仅删除本地 VLAN
- 转发通告
- 不进行同步

327P 078

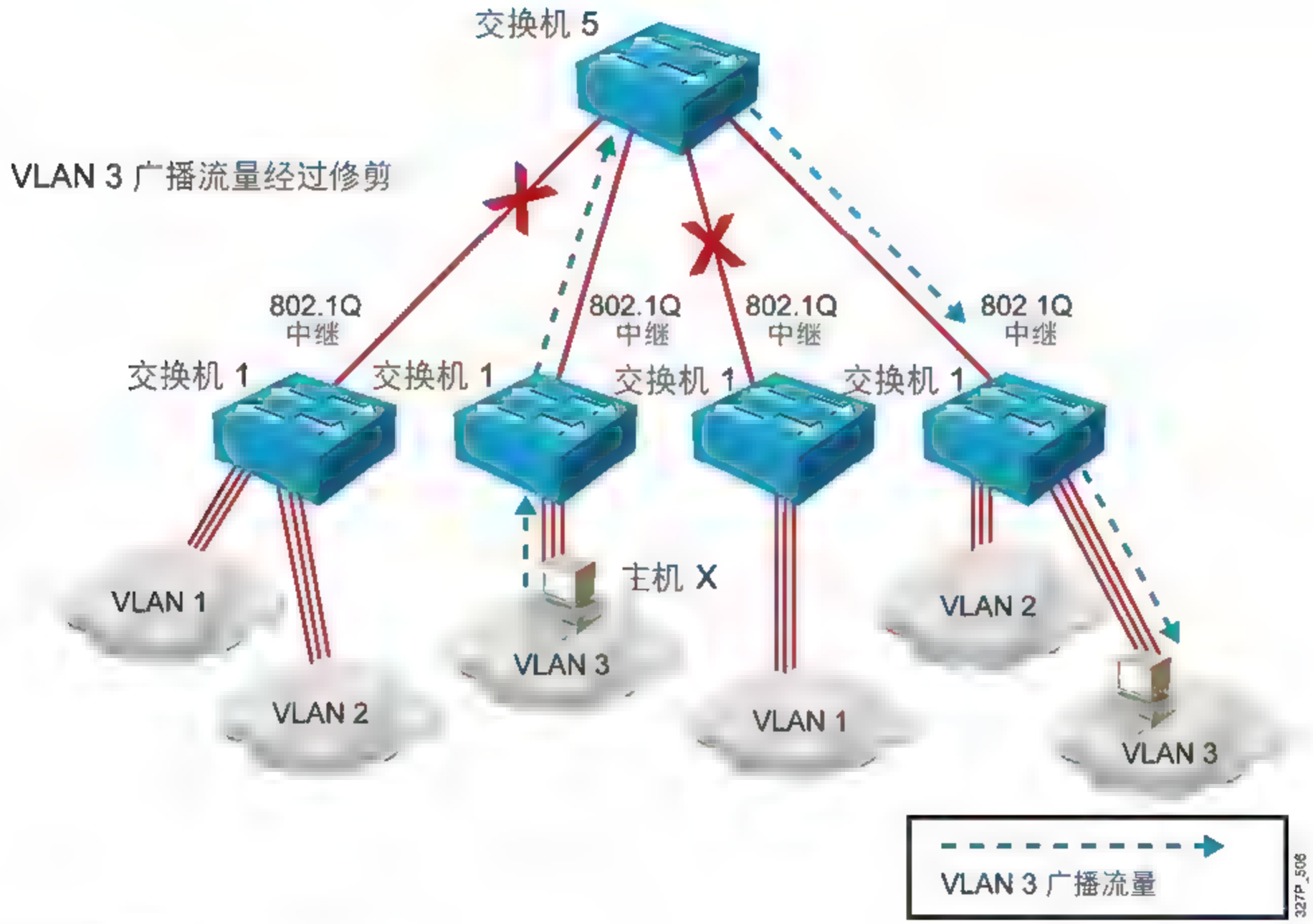
© 2008 Cisco Systems, Inc. 保留所有权利。

VTP 运行

- VTP 通告作为组播帧进行发送。
- VTP 服务器和客户端将同步到最新的修订版。
- VTP 通告每 5 分钟发送一次，或者当发生变更时发送。



VTP 修剪



© 2008 Cisco Systems, Inc. 保留所有权利。

配置 VLAN 和中继

1. 配置和检验 VTP。
2. 配置和检验 802.1Q 中继。
3. 在 VTP 服务器交换机上创建或修改 VLAN。
4. 将交换机端口分配到 VLAN 并进行检验。
5. 执行添加、移动和更改。
6. 保存 VLAN 配置。

© 2008 Cisco Systems, Inc. 保留所有权利

VTP 配置的指导原则

- Cisco Catalyst 交换机的默认 VTP 配置：
  - VTP 域名：无
  - VTP 模式：服务器模式
  - VTP 修剪：启用或禁用（特定于型号）
  - VTP 口令：空
  - VTP 版本：第 1 版
- 新交换机收到来自服务器的通告之后，可自动成为域的一部分。
- 如果客户端具有更高的修订版号，VTP 客户端将覆盖 VTP 服务器数据库。
- 域名分配了之后就无法删除；只能再重新分配。

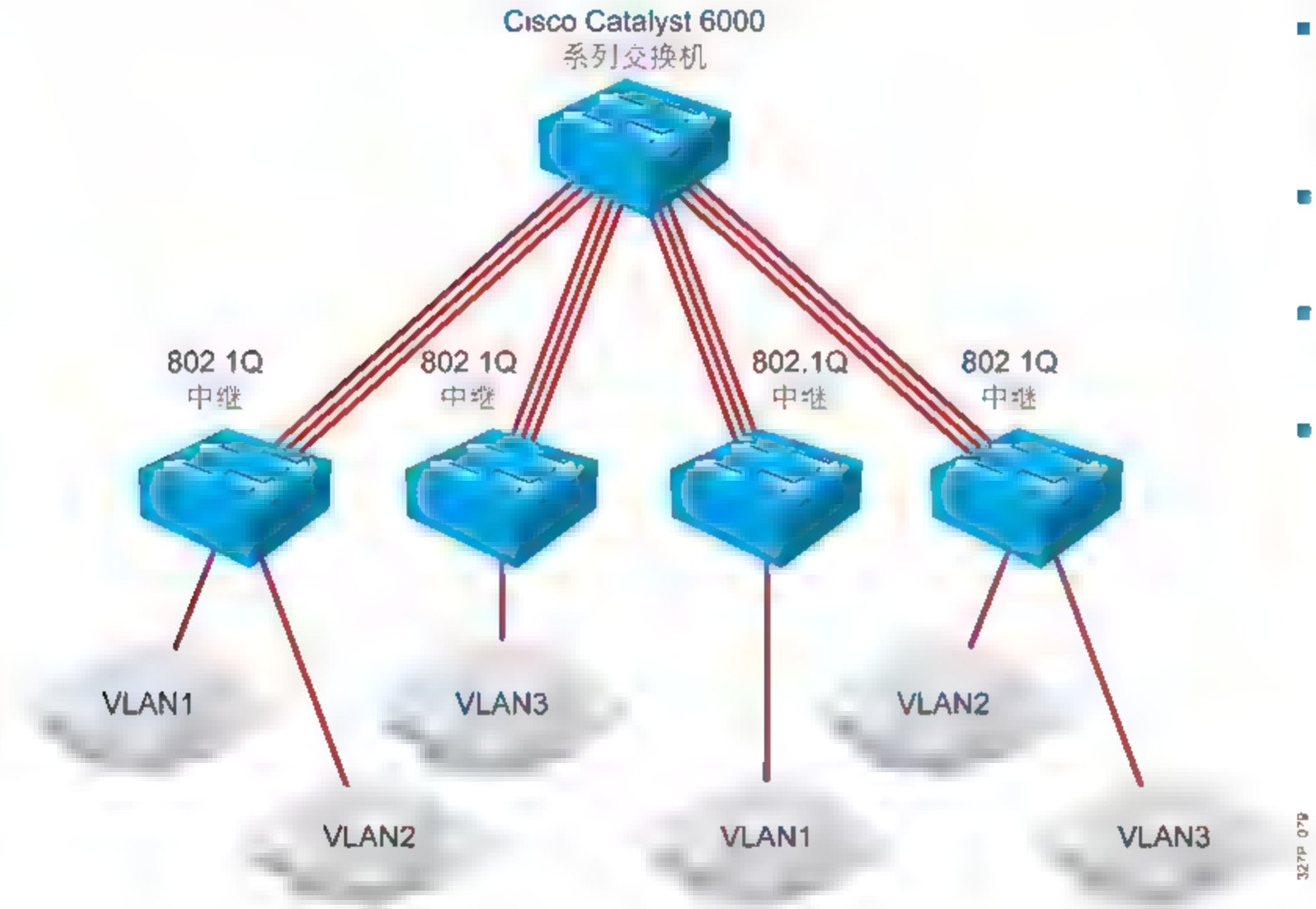
创建 VTP 域

```
SwitchX# configure terminal
SwitchX(config)# vtp mode [ server | client | transparent ]
SwitchX(config)# vtp domain domain-name
SwitchX(config)# vtp password password
SwitchX(config)# vtp pruning
SwitchX(config)# end
```

VTP 配置和验证示例

```
SwitchX(config)# vtp domain ICND
Changing VTP domain name to ICND
SwitchX(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
SwitchX(config)# end

SwitchX# show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 17
VTP Operating Mode              :Transparent
VTP Domain Name                 :ICND
VTP Pruning Mode                :Disabled
VTP V2 Mode                     :Disabled
VTP Traps Generation            :Disabled
MD5 digest                      :0x7D 0x6E 0x5E 0x3D 0xAF 0xA0 0x2F 0xAA
Configuration last modified by 10.1.1.4 at 3-3-93 20:08:05
SwitchX#
```

802.1Q 中继问题



- 确保中继链路两端的 802.1Q 中继的本征 VLAN 相同。
- 请注意，本征 VLAN 帧是无标记帧。
- 中继端口不能是安全端口。
- 一个 EtherChannel 组中所有 802.1Q 中继端口的配置必须相同。

配置 802.1Q 中继

```
SwitchX(config-if)#
switchport mode {access |  dynamic {auto | desirable} | trunk}
```

- 配置端口的中继特征

```
SwitchX(config-if)#
switchport mode trunk
```

- 将端口配置为 VLAN 中继

检验中继

```
SwitchX# show interfaces interface [switchport | trunk]
```

```
SwitchX# show interfaces fa0/11 switchport
Name:Fa0/11
Switchport:Enabled
Administrative Mode:trunk
Operational Mode:down
Administrative Trunking Encapsulation:dot1q
Negotiation of Trunking:On
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
 . . .
```

```
SwitchX# show interfaces fa0/11 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/11      desirable    802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/11      1-4094

Port        Vlans allowed and active in management domain
Fa0/11      1-13
```

VLAN 创建的指导原则

- VLAN 的最大数目取决于交换机。
- 大部分 Cisco Catalyst 桌面交换机都支持 128 个单独的生成树实例，每个 VLAN 一个生成树实例。
- VLAN 1 是出厂默认的以太网 VLAN。
- Cisco 发现协议和 VTP 通告将在 VLAN 1 上发送。
- Cisco Catalyst 交换机的 IP 地址位于管理 VLAN 中（默认为 VLAN 1）。
- 如果使用 VTP，交换机必须处于 VTP 服务器模式或透明模式才能添加或删除 VLAN。

添加 VLAN

```
SwitchX# configure terminal
SwitchX(config)# vlan 2
SwitchX(config-vlan)# name switchlab99
```

检验 VLAN

```
SwitchX# show vlan [brief | id vlan-id || name vlan-name]
```

```
SwitchX# show vlan id 2

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
2    switchlab99                         active    Fa0/2, Fa0/12

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

.    .    .
SwitchX#
```

分配交换机端口到 VLAN

```
SwitchX(config-if)#
```

```
switchport access [vlan vlan# | dynamic]
```

```
SwitchX# configure terminal
SwitchX(config)# interface range fastethernet 0/2 - 4
SwitchX(config-if)# switchport access vlan 2

SwitchX# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                           active    Fa0/1
2    switchlab99                       active    Fa0/2, Fa0/3, Fa0/4
```

检验 VLAN 成员资格

```
SwitchX# show vlan brief
```

```
SwitchX# show vlan brief
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                              active    Fa0/1
2    switchlab99                          active    Fa0/2, Fa0/3, Fa0/4
3    vlan3                                active
4    vlan4                                active
1002 fddi-default                         act/unsup
1003 token-ring-default                   act/unsup

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1004 fddinet-default                      act/unsup
1005 trnet-default                        act/unsup
```

检验 VLAN 成员资格（续）

Switch#

```
show interfaces interface switchport
```

```
SwitchX# show interfaces fa0/2 switchport
Name:Fa0/2
Switchport:Enabled
Administrative Mode:dynamic auto
Operational Mode:static access
Administrative Trunking Encapsulation:dot1q
Operational Trunking Encapsulation:native
Negotiation of Trunking:On
Access Mode VLAN:2 (switchlab99)
Trunking Native Mode VLAN:1 (default)
--- 省略部分输出 ----
```

VLAN 的添加、移动和更改操作

- 如果使用 VTP，交换机必须处于 VTP 服务器模式或透明模式才能添加或删除 VLAN。
- 当您通过处于 VTP 服务器模式的交换机来更改 VLAN 时，所做更改会传播至 VTP 域中的其它交换机。
- 更改 VLAN 通常意味着更改了 IP 网络。
- 将端口重新分配给新的 VLAN 之后，该端口将自动从先前的 VLAN 中删除。
- 删除 VLAN 后，该 VLAN 中所有未移动到活动 VLAN 的端口都将无法与其它工作站通信。

总结

- 设计欠佳的网络会增加支持成本并降低服务可用性，而且会限制对新应用程序和解决方案的支持。
- VLAN 可灵活地进行分段和组织。
- 以太网中继通过一条链路传输多个 VLAN 的流量，并允许 VLAN 跨越整个网络。
- VTP 是维护 VLAN 配置一致性的第 2 层消息协议。

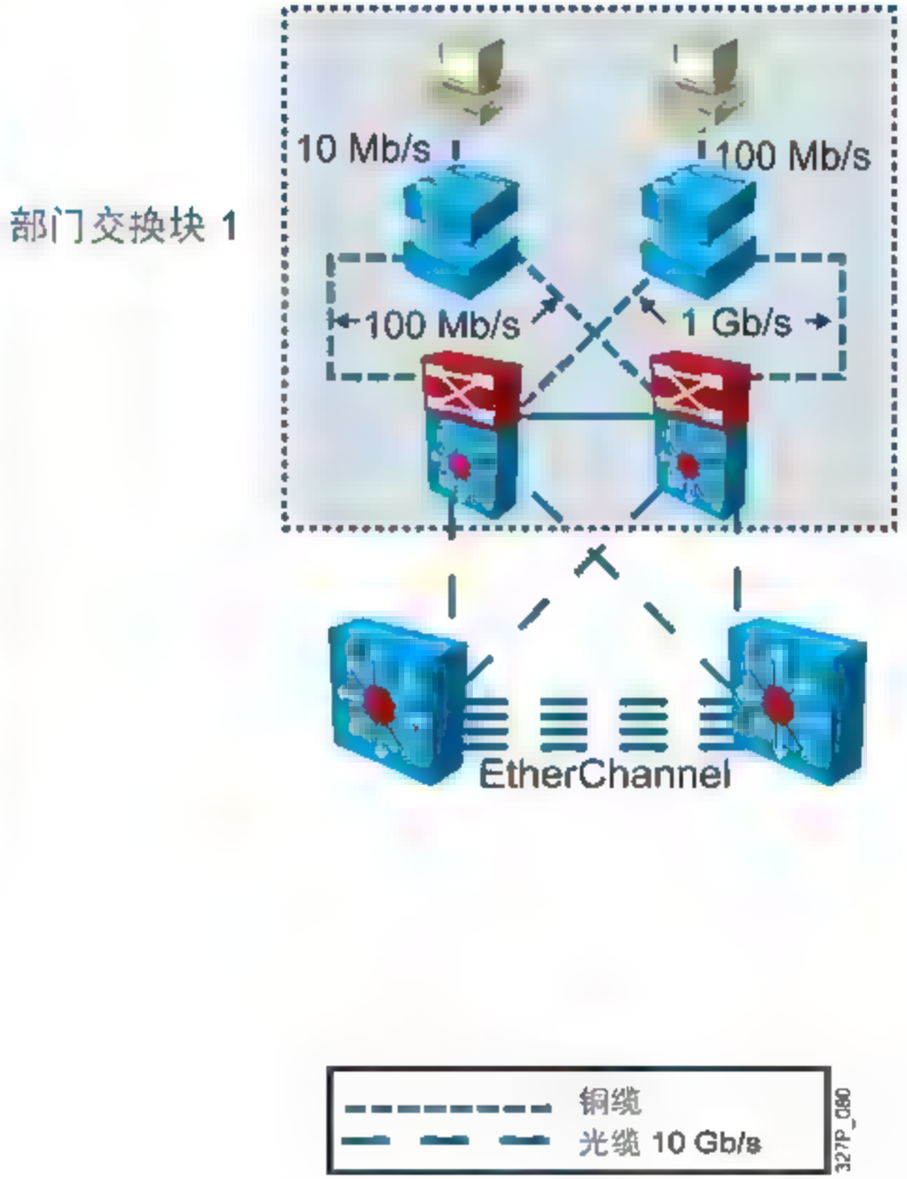
CISCO

使用生成树来提高性能

中型交换网络结构

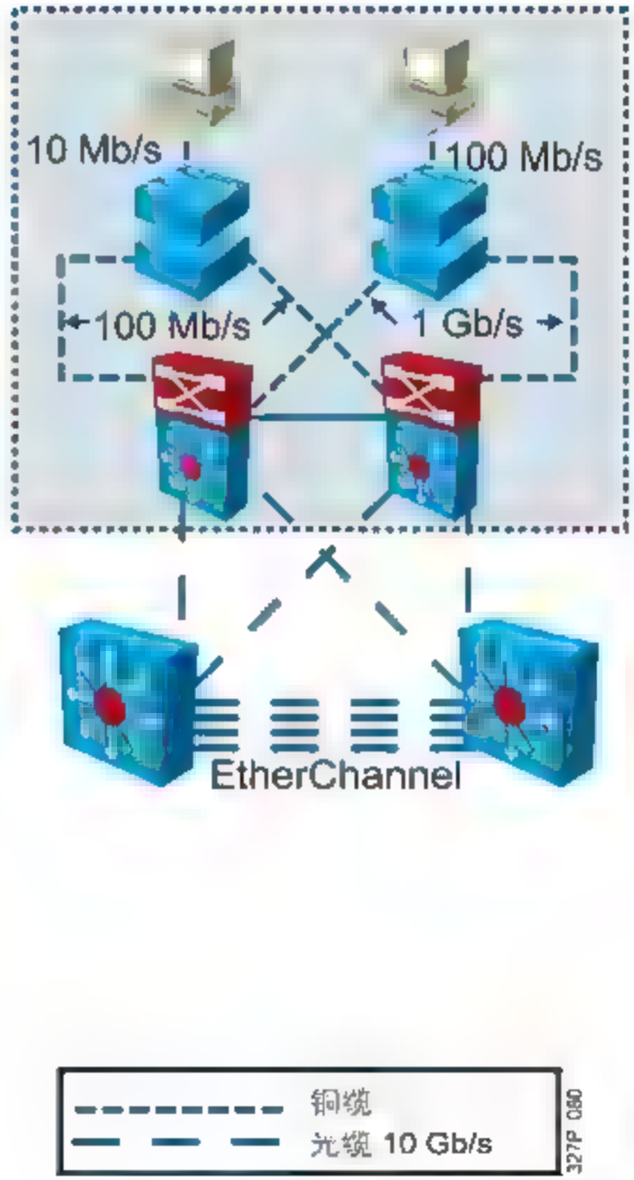
互连技术

技术	用途
FastEthernet	将最终用户设备连接到接入层交换机
千兆以太网	将接入交换机连接到分布层交换机，以及将负载较高的服务器连接到交换机
万兆以太网	为交换链路和主干提供高速交换
EtherChannel	利用冗余为交换链路和主干提供高速交换



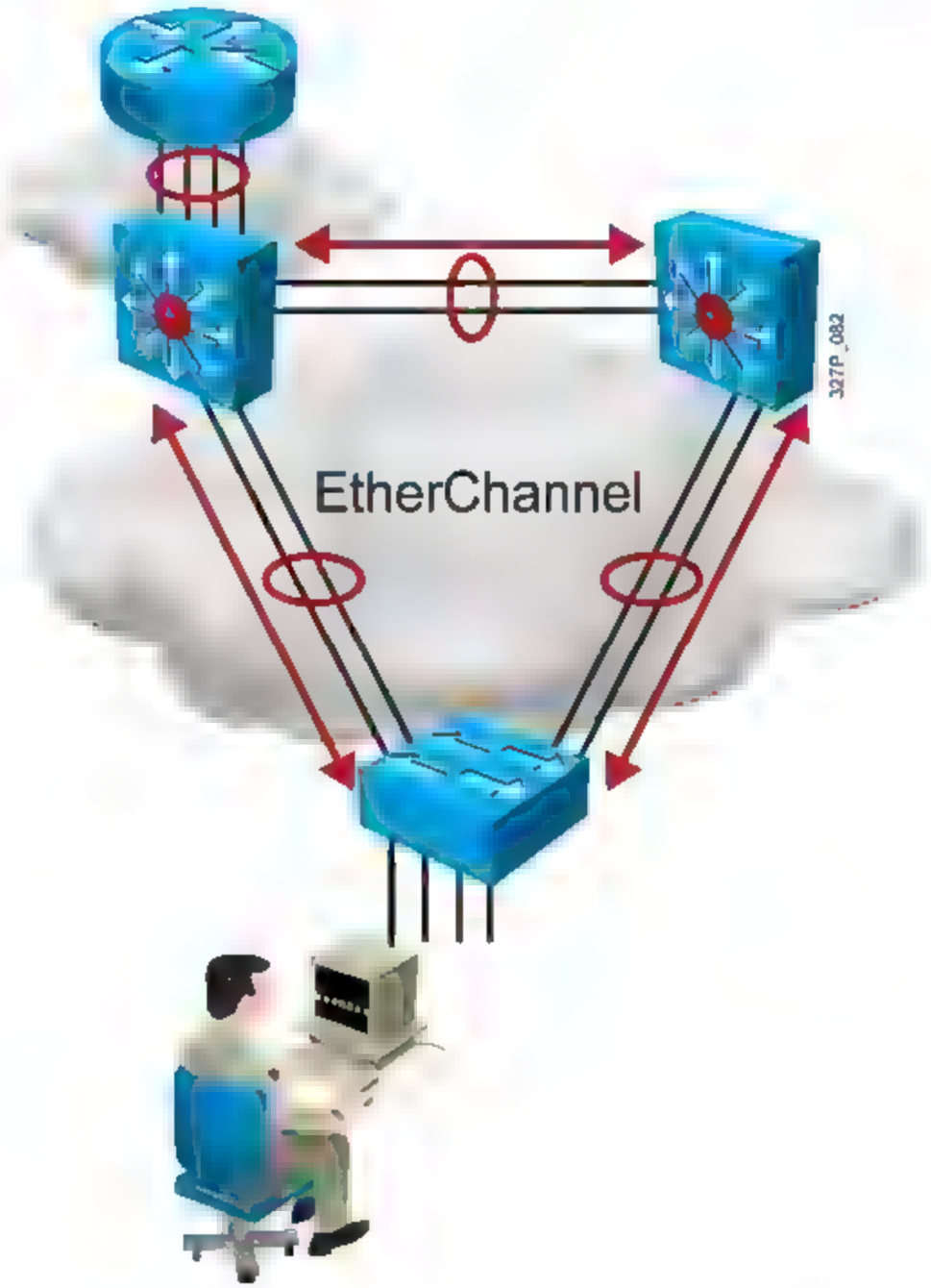
确定需要的设备和布线

每条链路都能为通过该链路的总聚合流量提供足够的带宽。

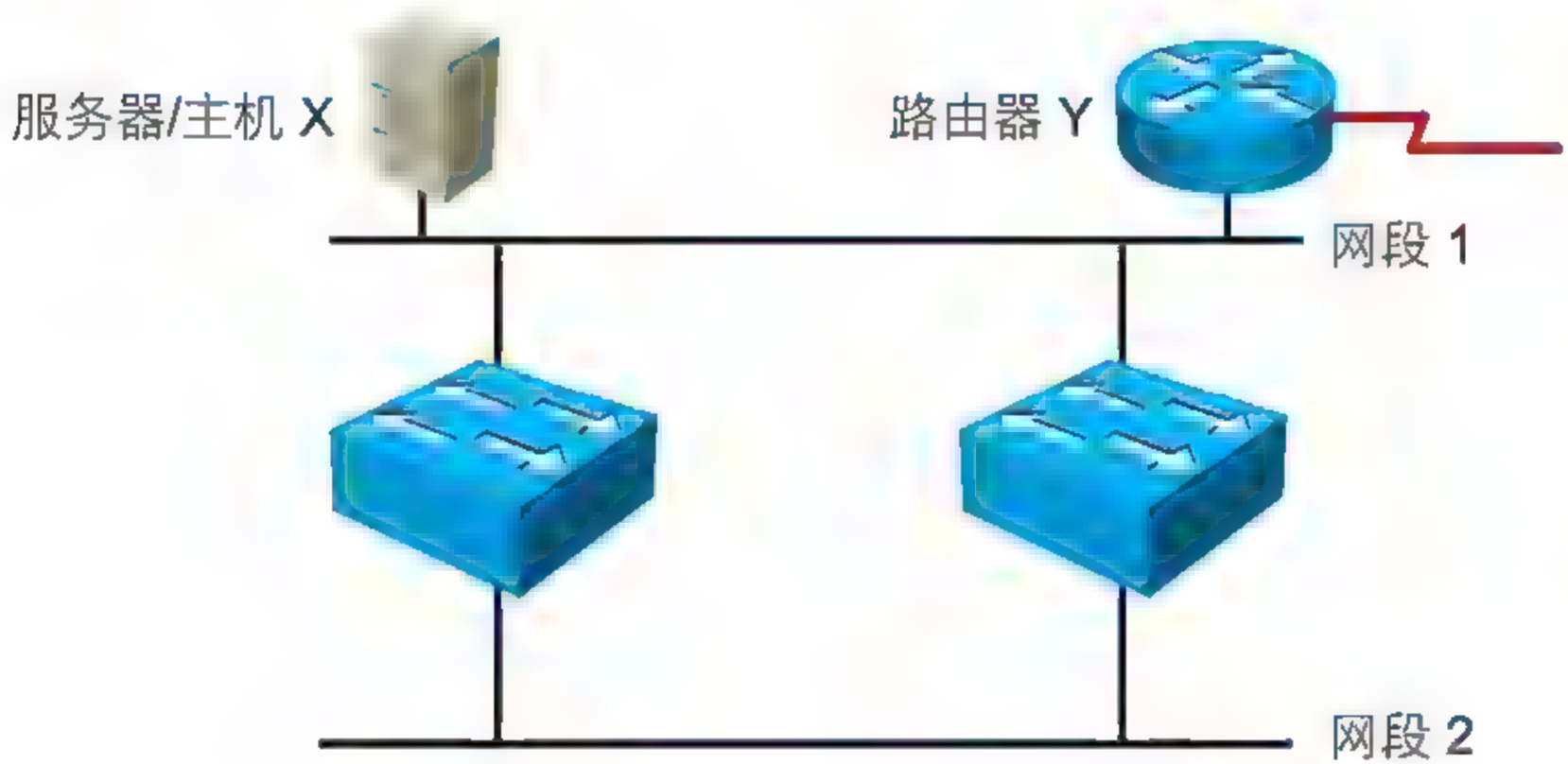


EtherChannel 的优点

- 交换机之间相似链路的逻辑聚合
- 链路间负载共享
- 视为一个 STP 逻辑端口
- 冗余

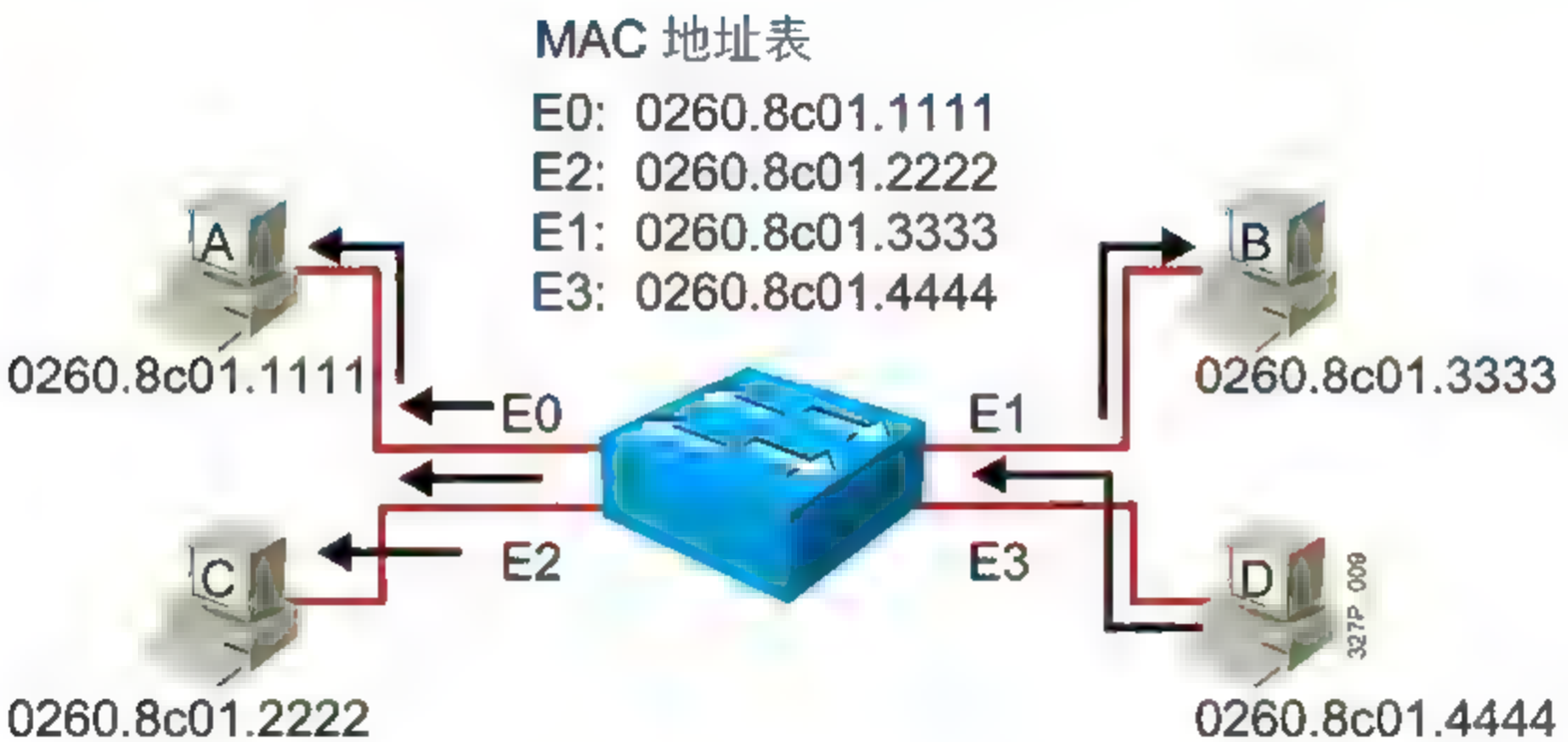


冗余拓扑



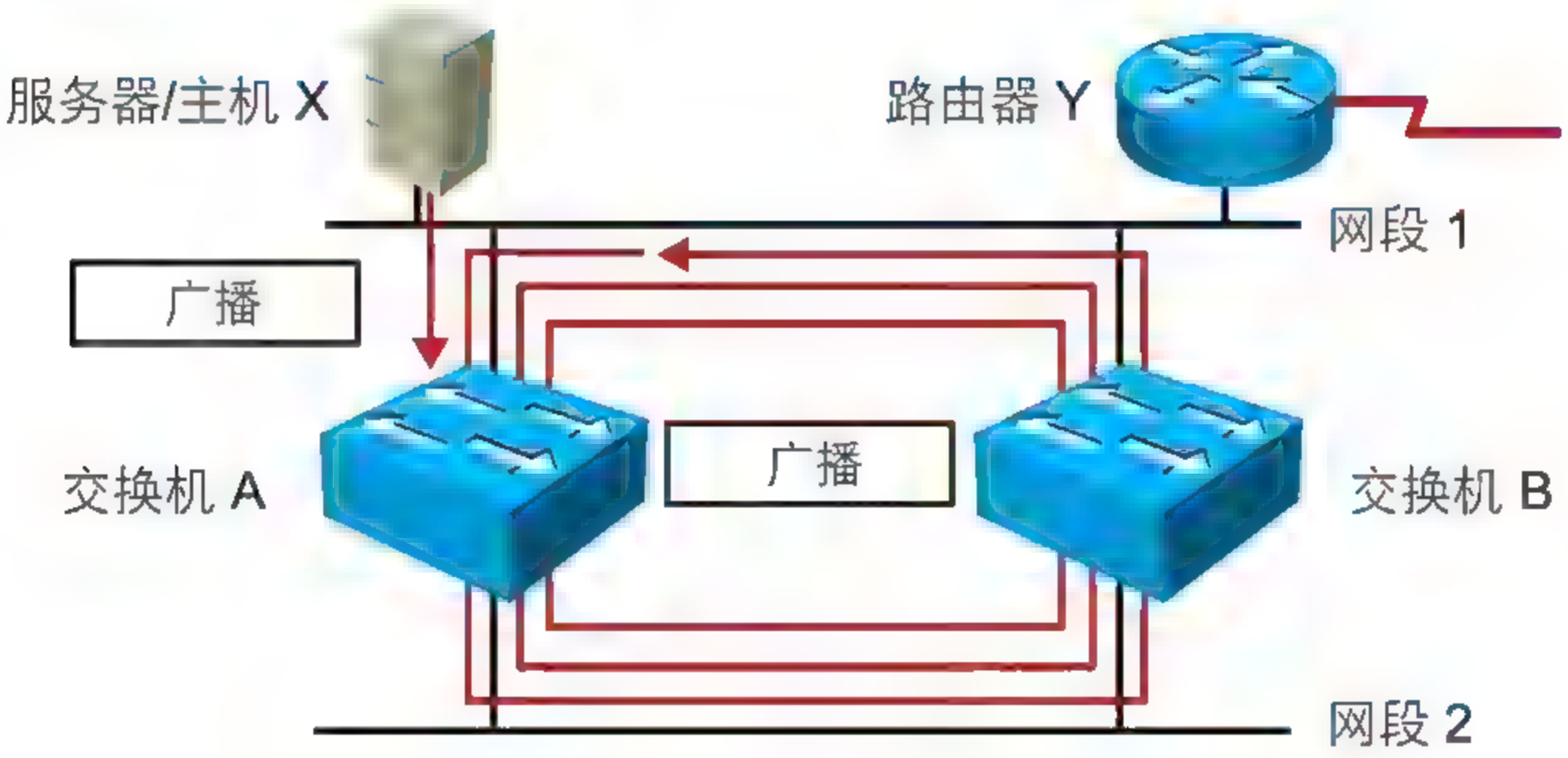
- 冗余功能可消除单点故障。
- 冗余拓扑会导致广播风暴、帧有多个副本以及 MAC 地址表不稳定。

广播帧



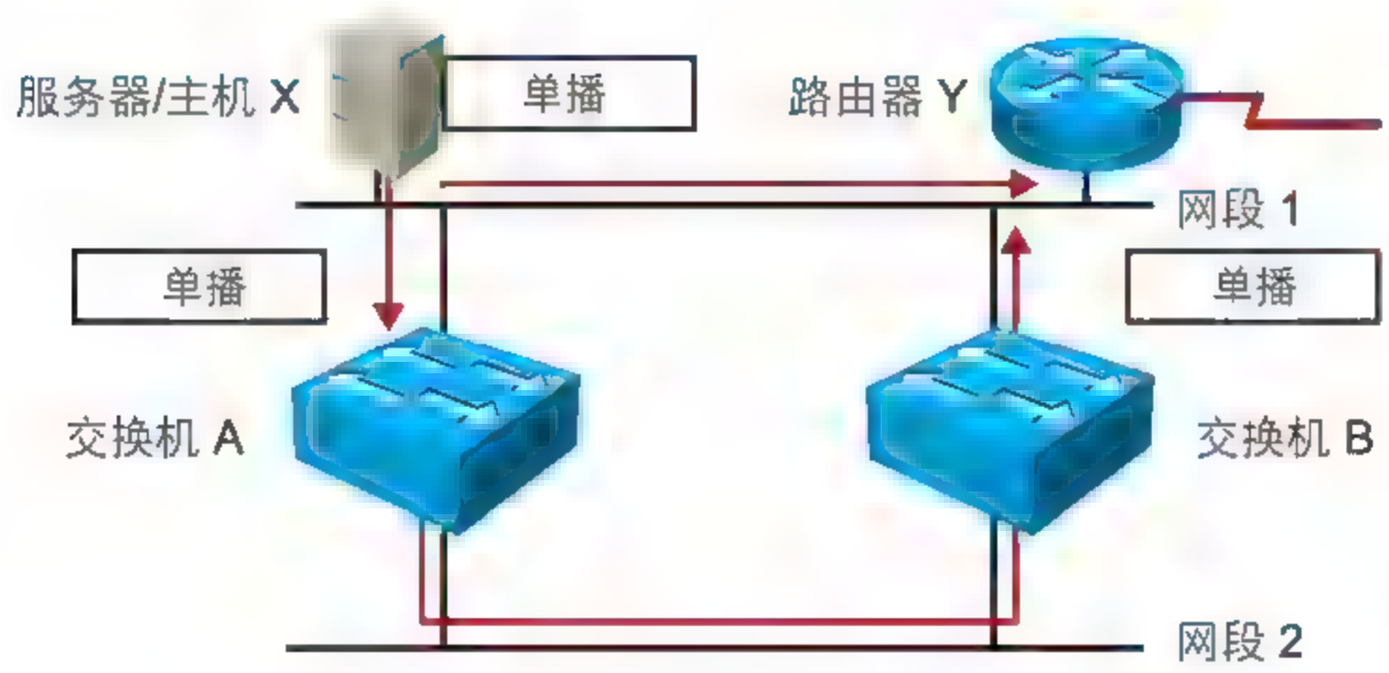
- 工作站 D 发送广播帧。
- 广播帧会泛洪到除始发端口之外的其它所有端口。

广播风暴



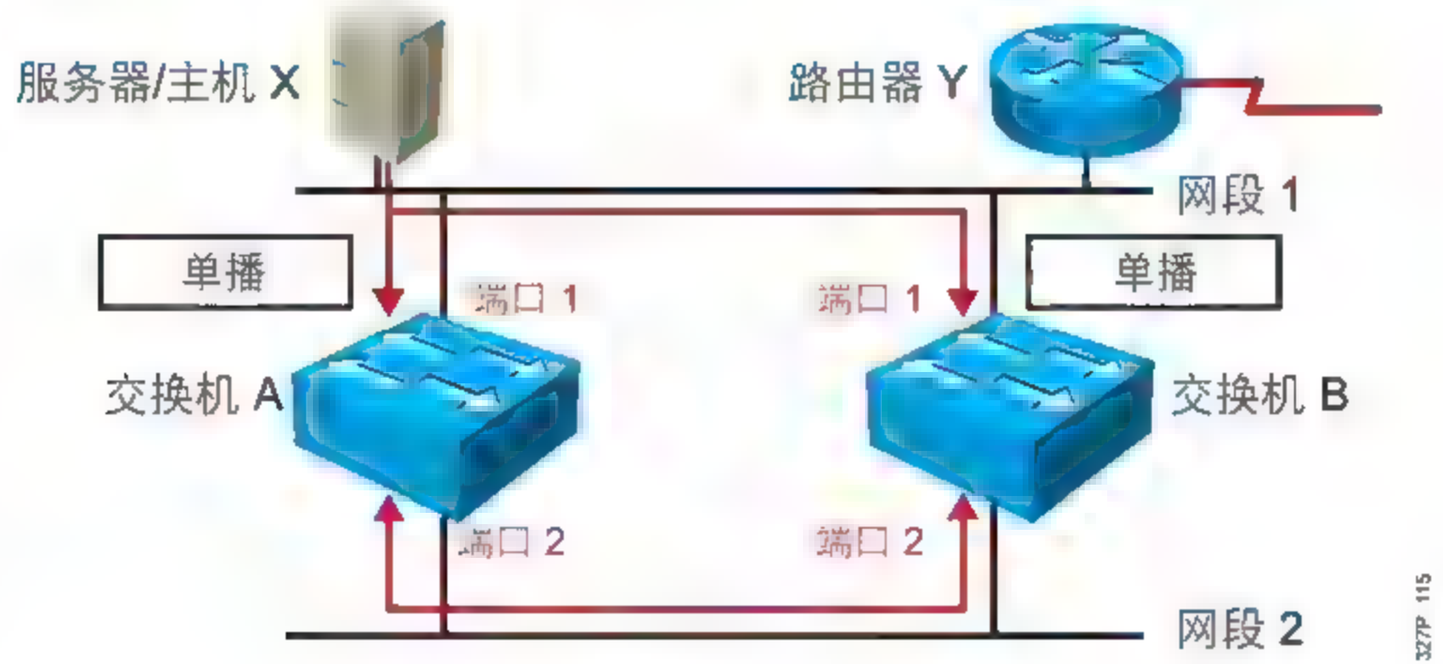
- 主机 X 发送广播。
- 交换机继续反复传播广播流量。

帧的多个副本



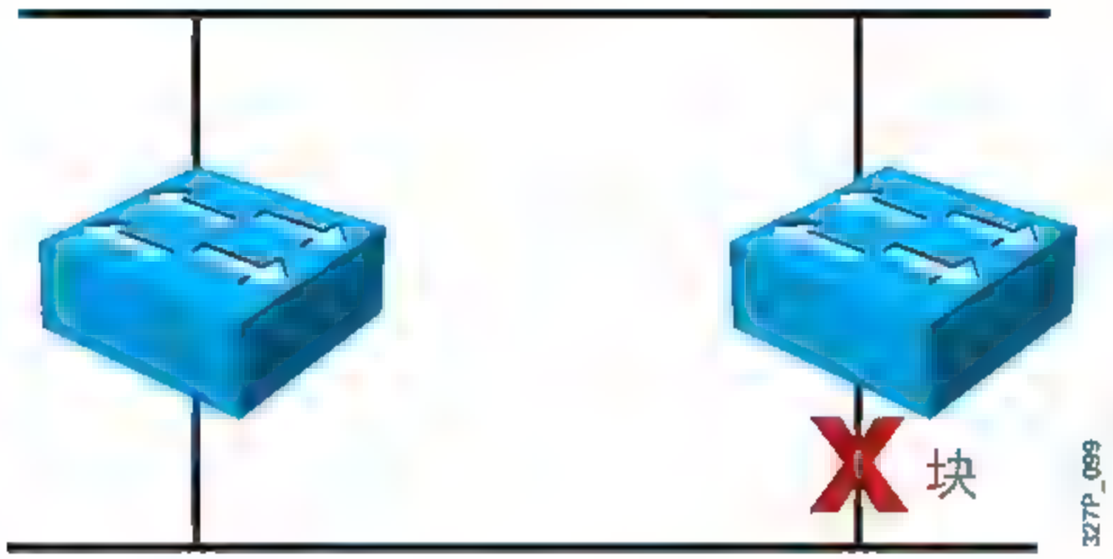
- 主机 X 将单播帧发往路由器 Y。
- 两台交换机均未获得路由器 Y 的 MAC 地址。
- 路由器 Y 将收到同一个帧的两个副本。

MAC 数据库的不稳定性



- 主机 X 将单播帧发往路由器 Y。
- 两台交换机均未获得路由器 Y 的 MAC 地址。
- 交换机 A 和 B 在端口 1 上获得主机 X 的 MAC 地址。
- 帧被泛洪到路由器 Y。
- 交换机 A 和交换机 B 在端口 2 上获得主机 X 的错误 MAC 地址。

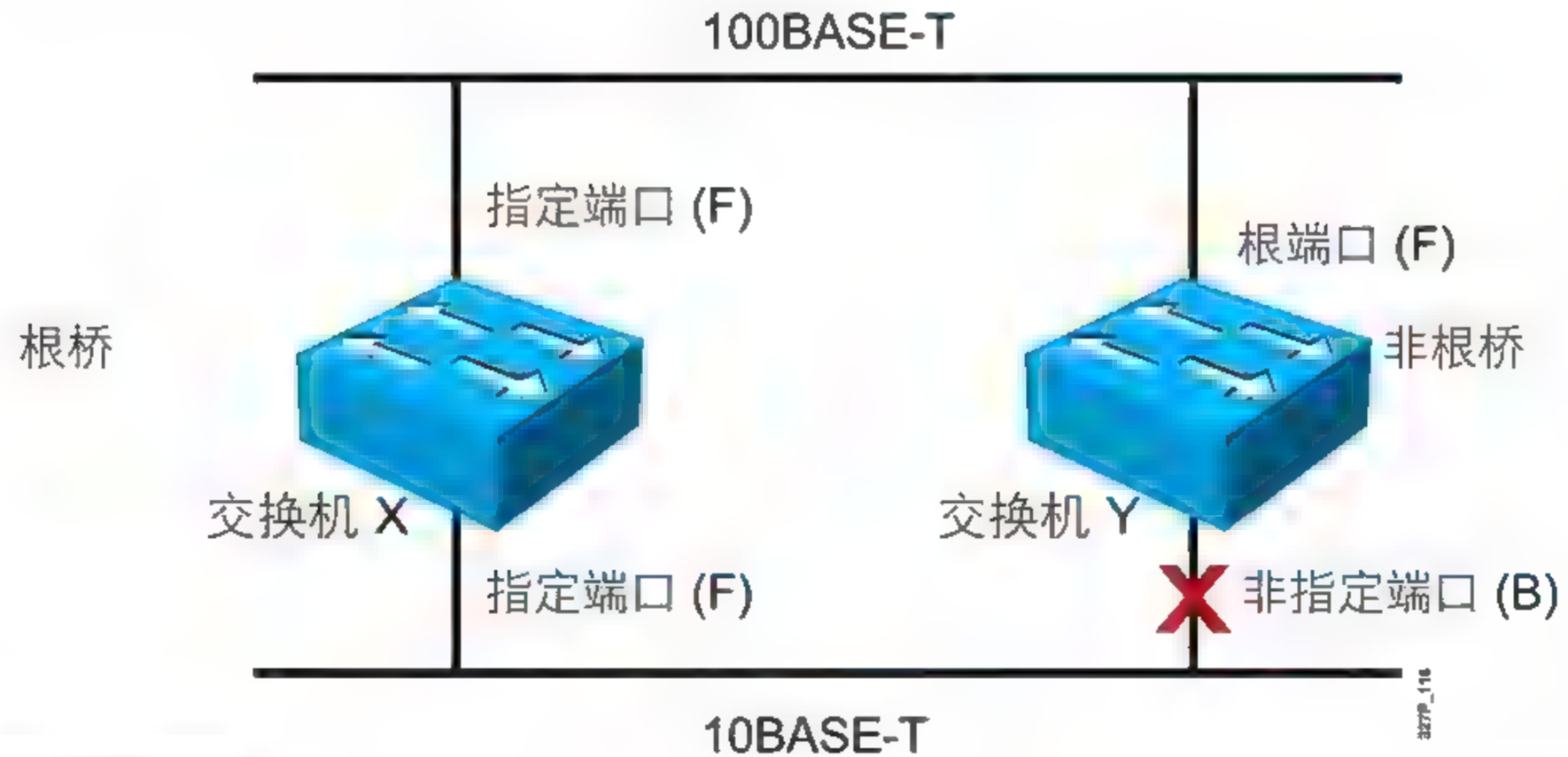
使用 STP 的环路解决方案



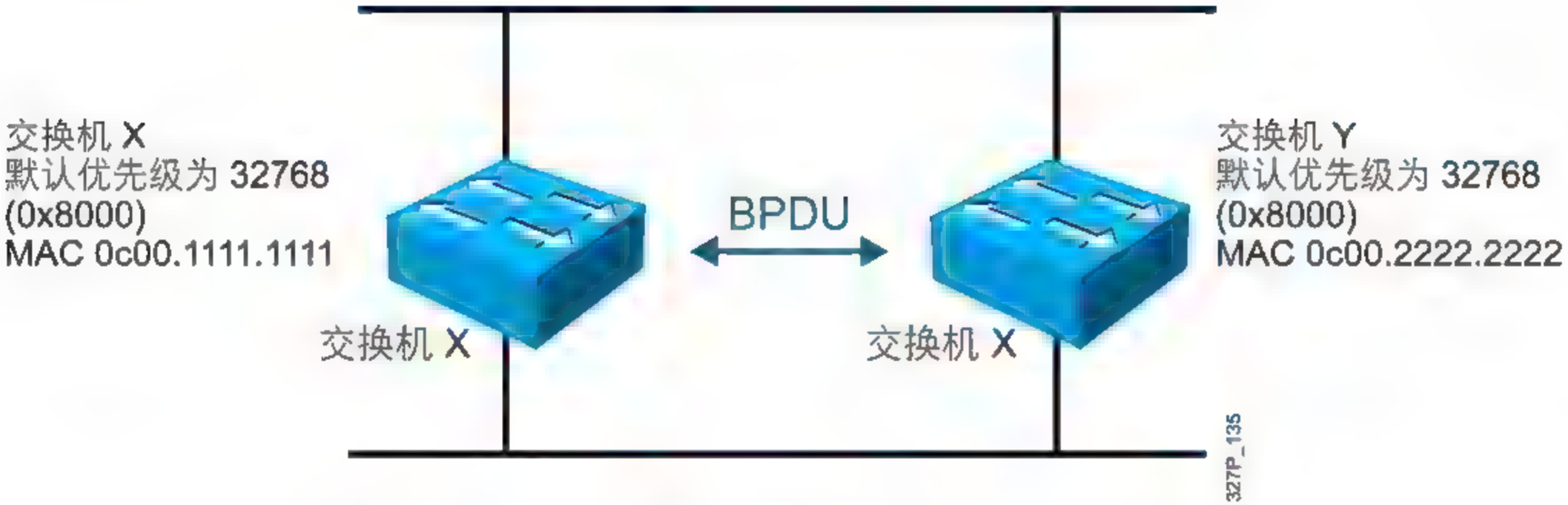
- 通过将某些端口置于阻塞状态提供无环路的冗余网络
- 在 IEEE 802.1D 规范中发布
- 通过实施 Cisco PVST+ 得以增强

生成树操作

- 每个广播域有一个根桥。
- 每个非根桥有一个根端口。
- 每个网段有一个指定端口。
- 不使用非指定端口。



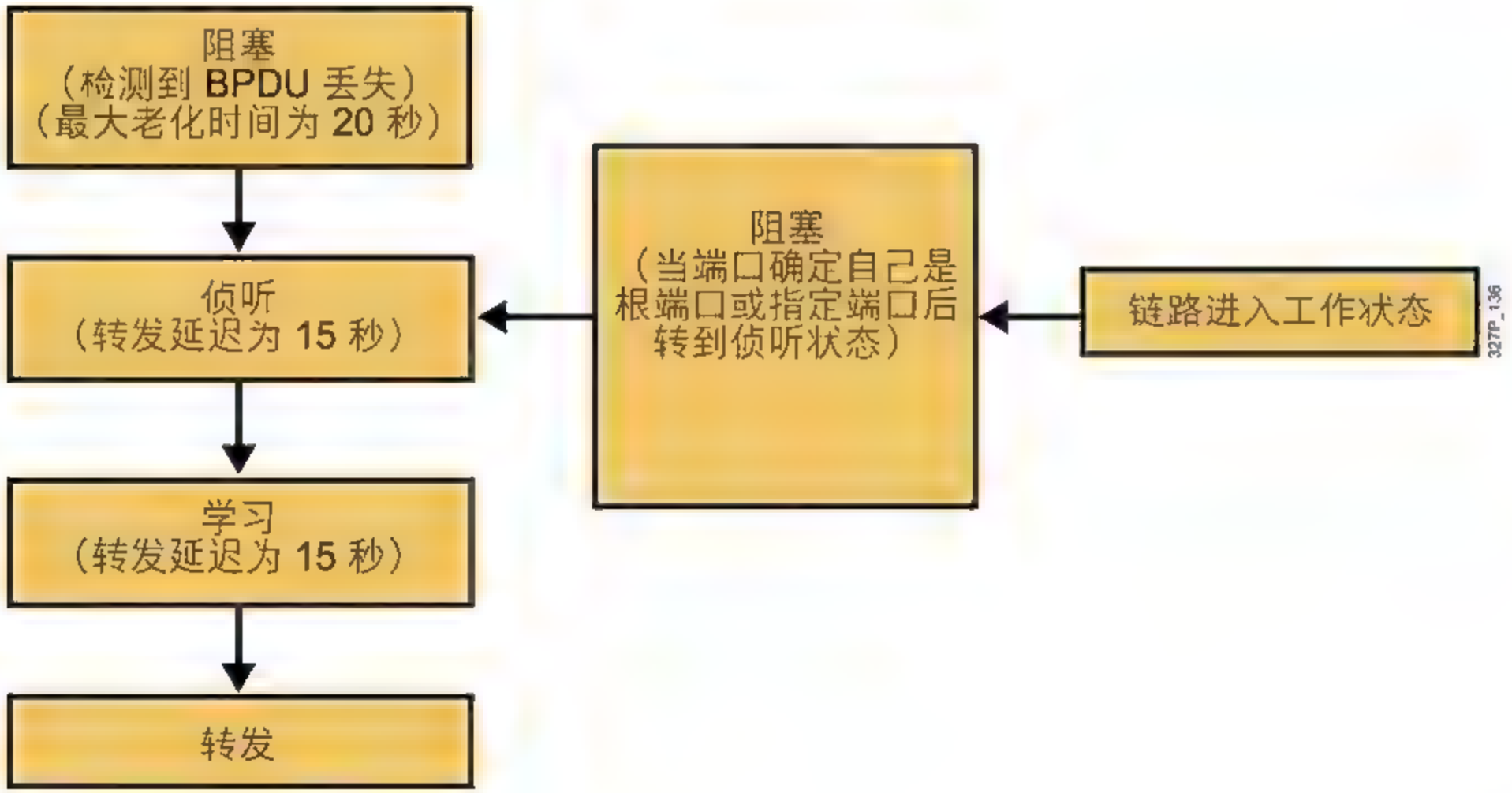
STP 根桥选择



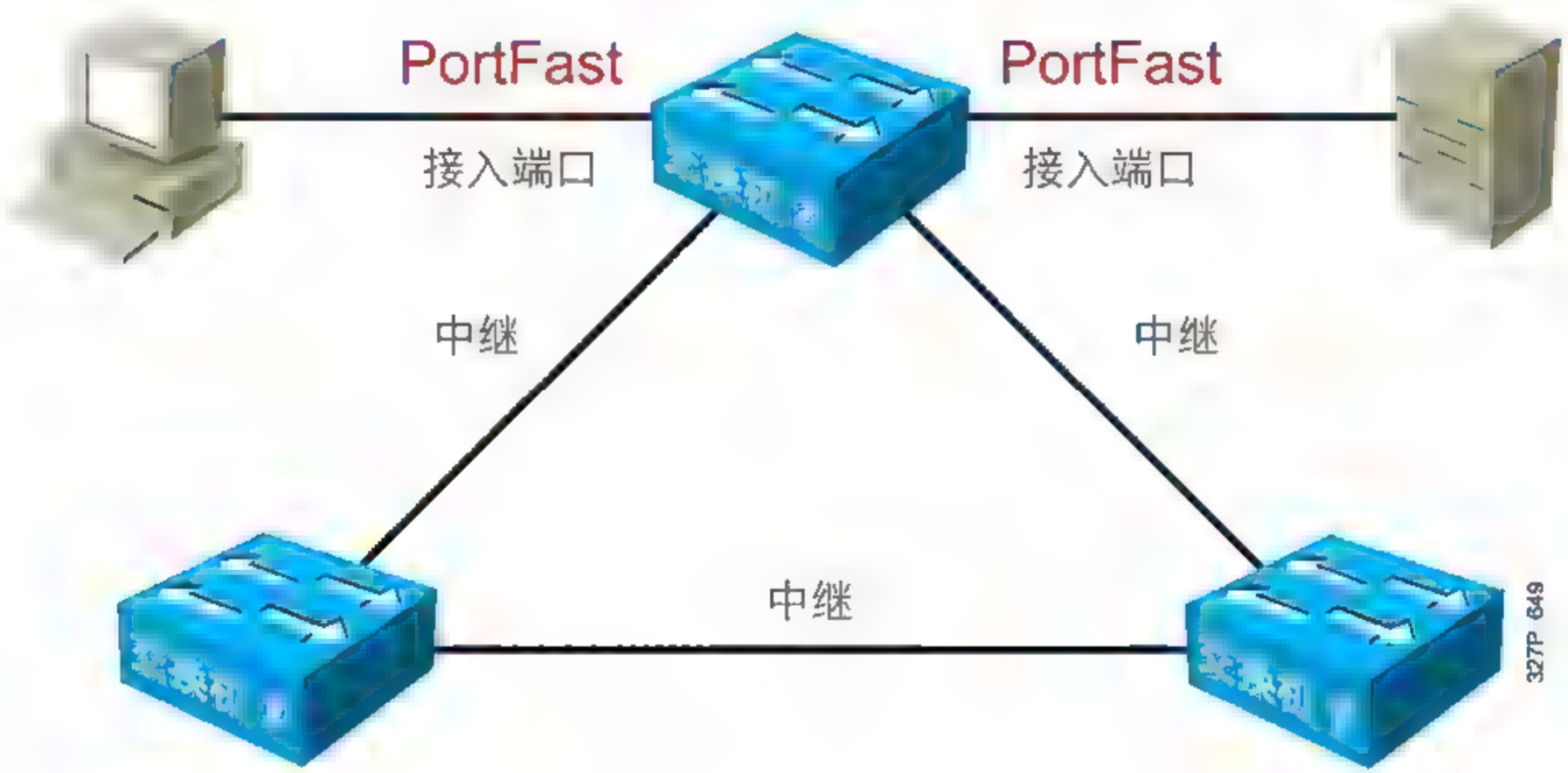
- BPDU（默认 = 每 2 秒发送一次）
- 根桥 = 网桥 ID 最小的网桥
- 网桥 ID = [网桥优先级] [MAC 地址]

生成树端口状态

生成树在几种不同的状态之间转换每个端口：



介绍 PortFast



PortFast 是在接入端口而非中继端口上配置的。

配置和检验 PortFast

```
SwitchX(config-if)#
spanning-tree portfast
```

- 在接口上配置 PortFast

或者

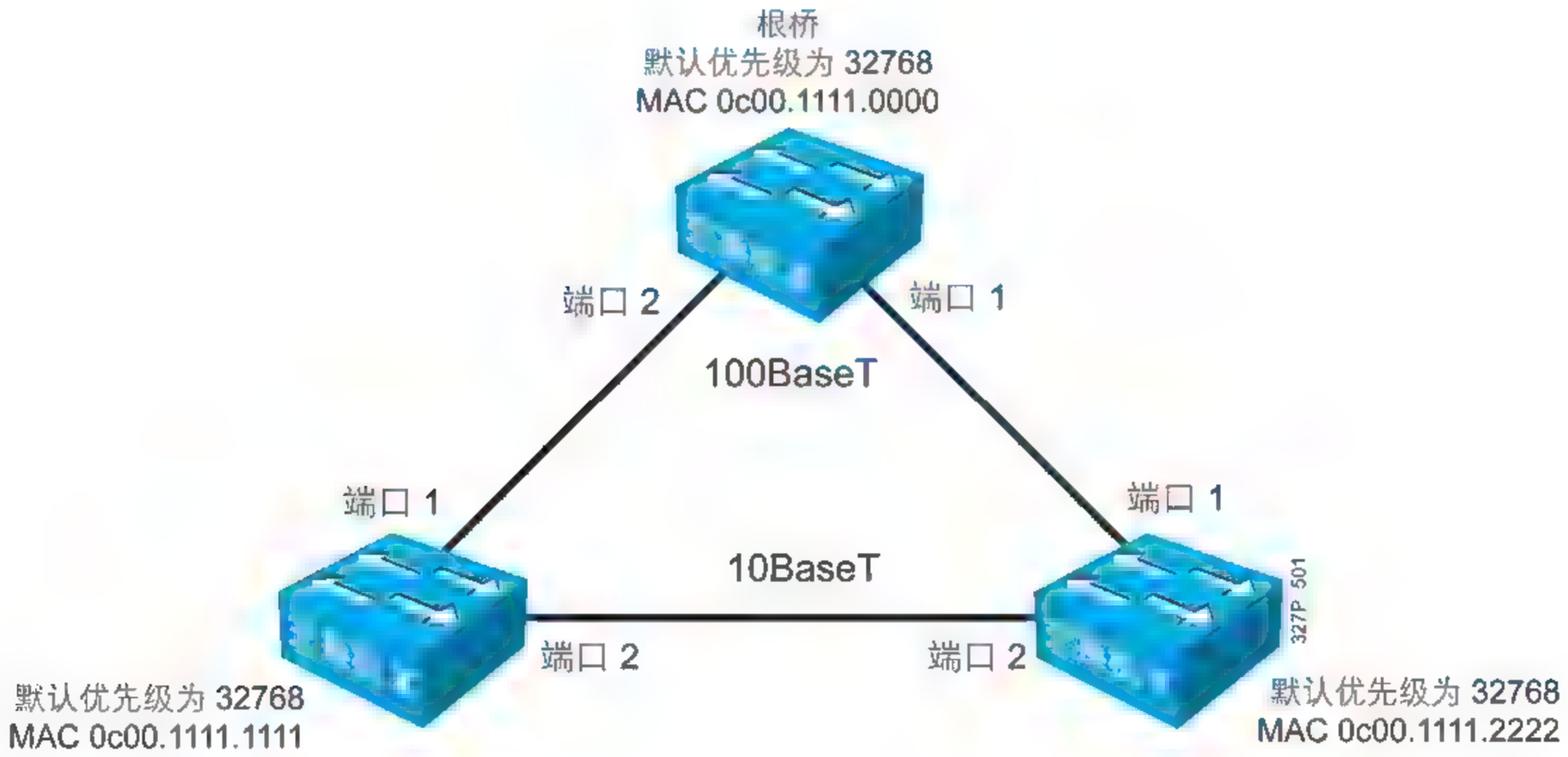
```
SwitchX(config)#
spanning-tree portfast default
```

- 在所有非中继接口上启用 PortFast

```
SwitchX#
show running-config interface interface
```

- 检验是否已在接口上配置了 PortFast

生成树操作示例



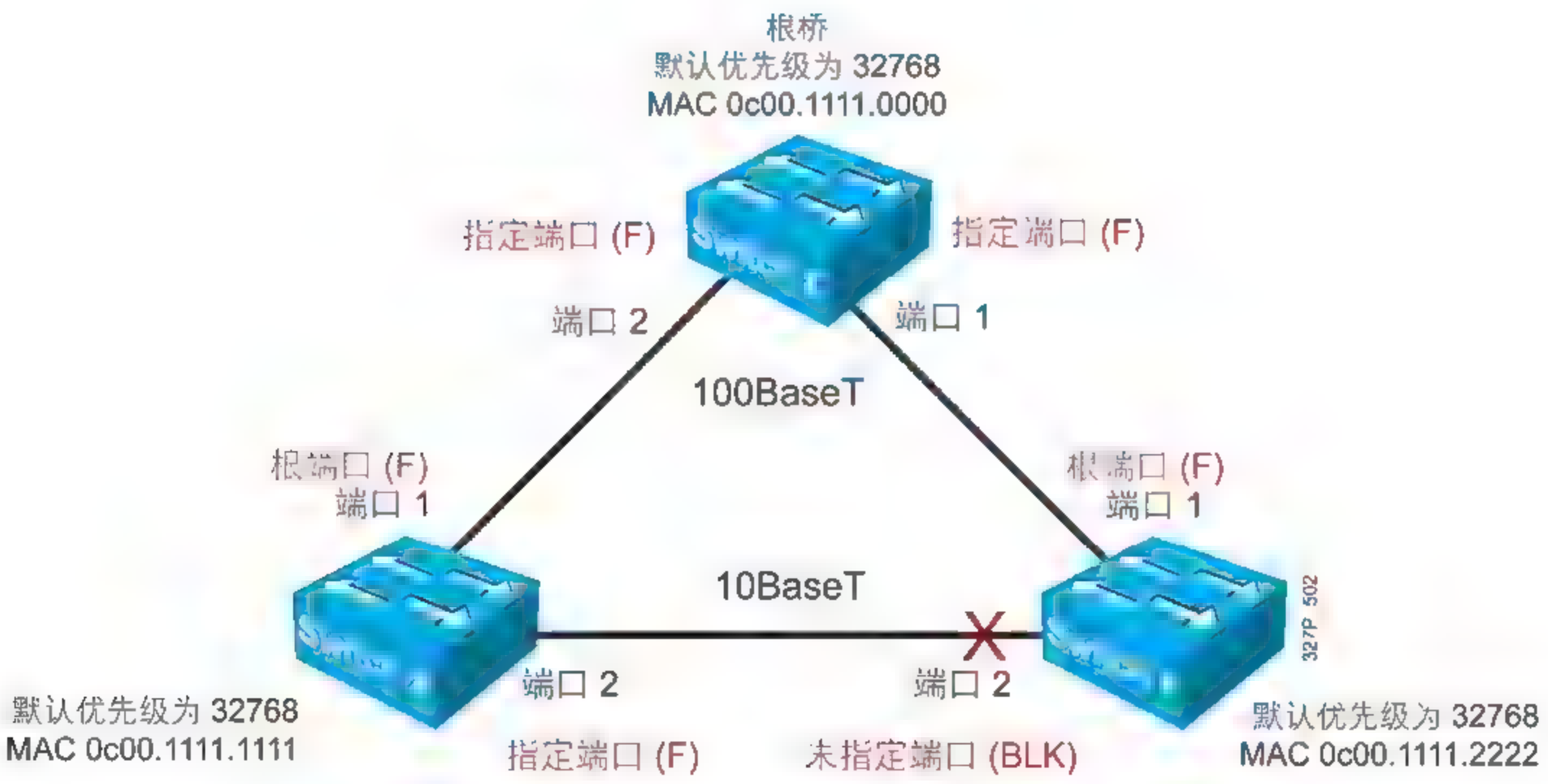
© 2008 Cisco Systems, Inc. 保留所有权利。

生成树路径开销

链路速度	开销（修订的 IEEE 规范）	开销（之前的 IEEE 规范）
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

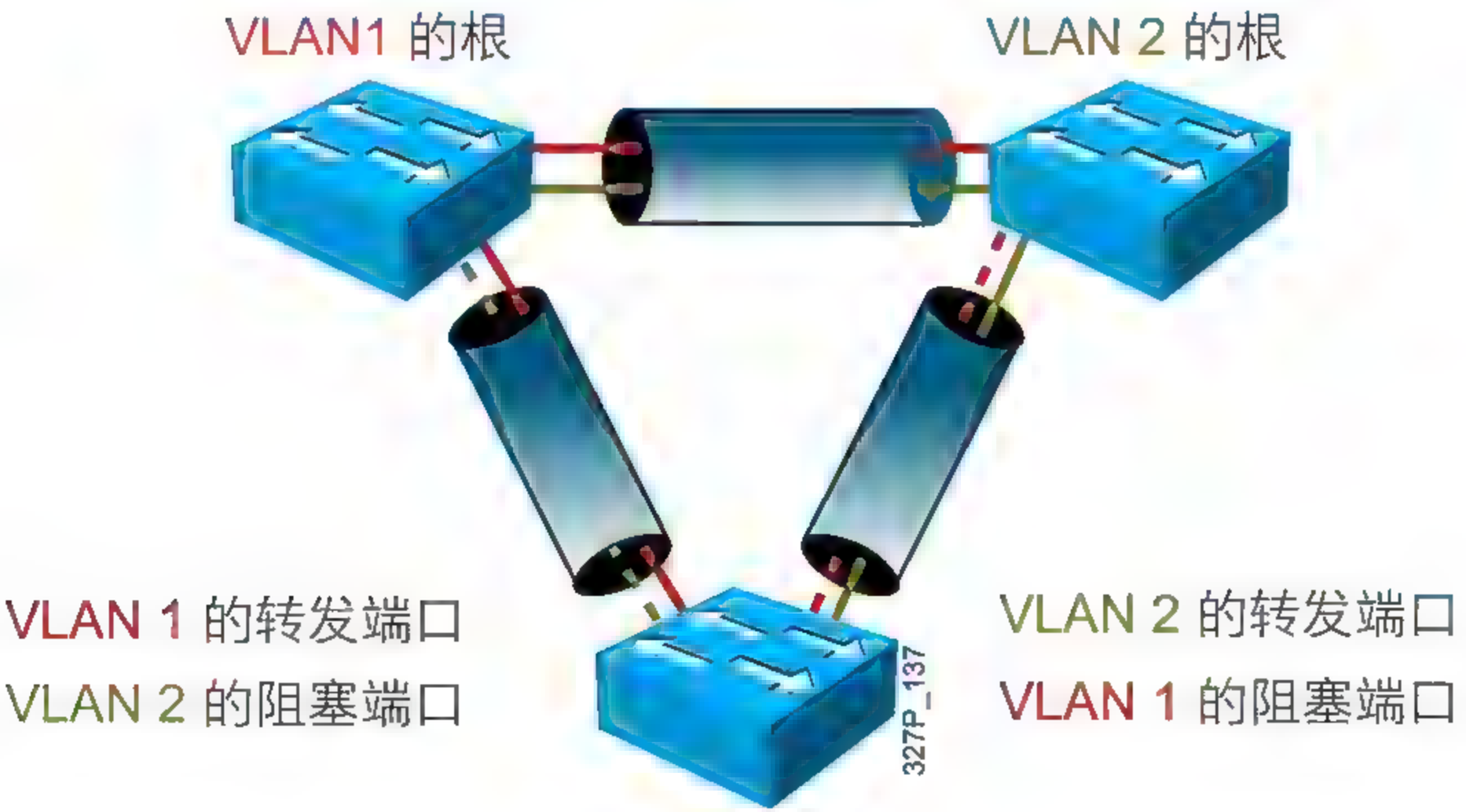
© 2008 Cisco Systems, Inc. 保留所有权利。

生成树重新计算



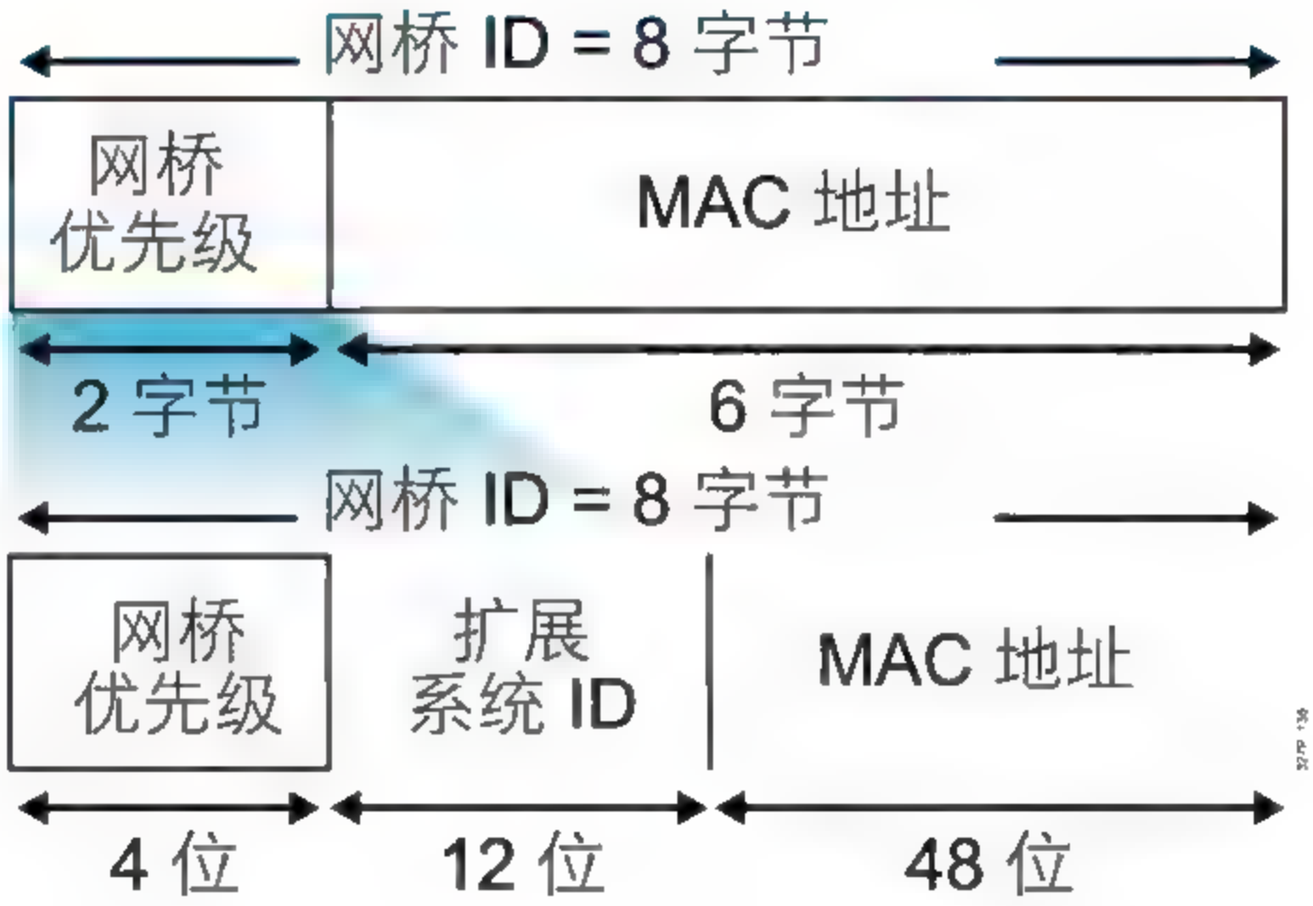
© 2008 Cisco Systems, Inc. 保留所有权利。

增强型每个 VLAN 生成树



PVST+ 扩展网桥 ID

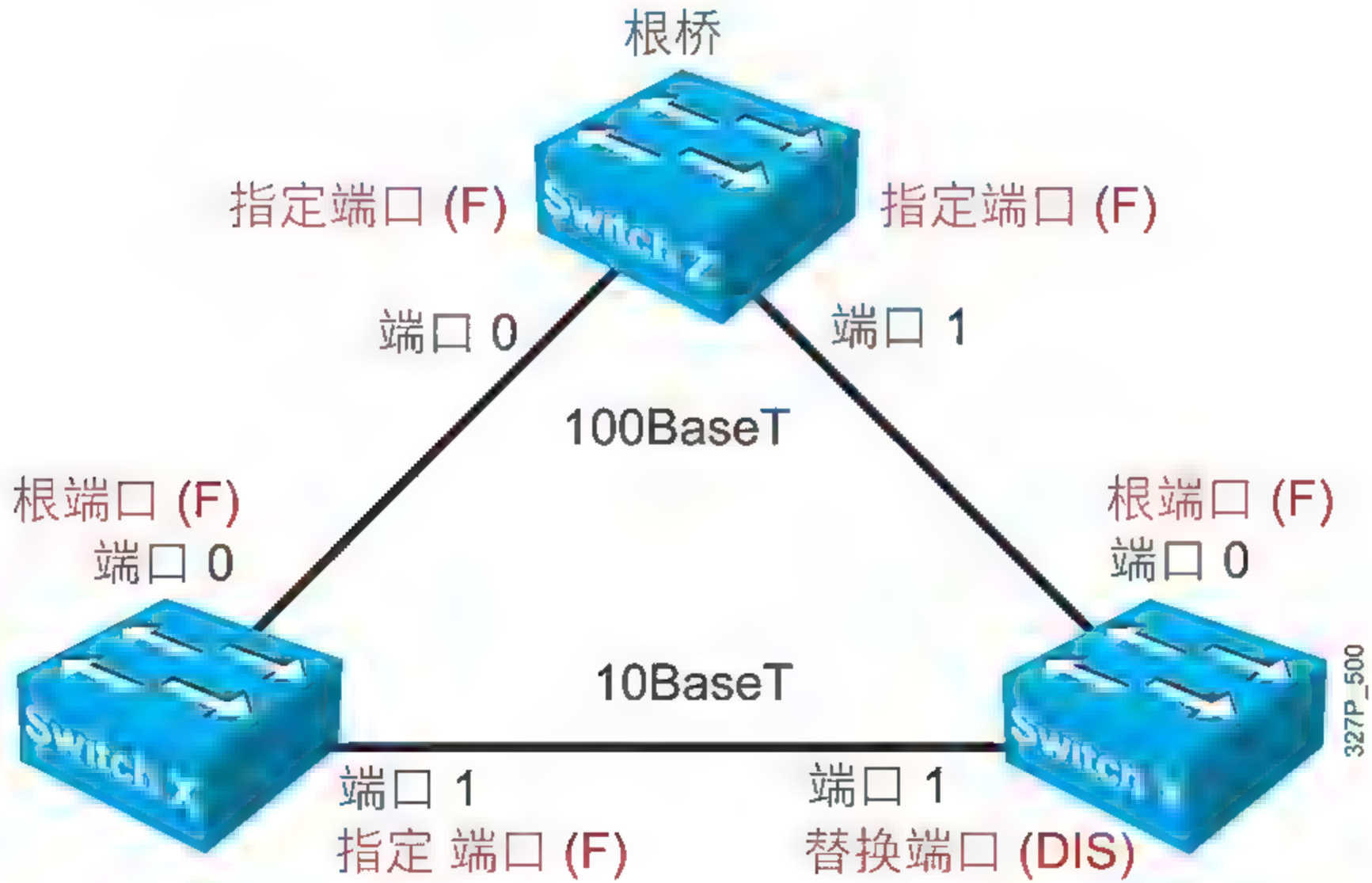
不带扩展系统 ID 的网桥 ID



带系统 ID 的扩展网桥 ID

系统 ID = VLAN

快速生成树协议


根桥
指定端口 (F)
指定端口 (F)
端口 0
端口 1
100BaseT
根端口 (F)
端口 0
根端口 (F)
端口 0
10BaseT
端口 1
指定 端口 (F)
端口 1
替换端口 (DIS)
327P_500

默认生成树配置

- Cisco Catalyst 交换机支持三种类型的 STP：
  - PVST+
  - PVRST+
  - MSTP
- Cisco Catalyst 交换机的默认 STP 是 PVST+：
  - 每个 VLAN 都有单独的 STP 实例
  - 所有 VLAN 只有一个根桥
  - 无负载共享

PVRST+ 配置的指导原则

1. 启用 PVRST+。
2. 将某一交换机指定为根桥，并对其进行配置。
3. 将某一交换机指定为次根桥，并对其进行配置。
4. 检验配置。

PVRST+ 实施命令

SwitchX(config)#

```
spanning-tree mode rapid-pvst
```

- 配置 PVRST+

SwitchX#

```
show spanning-tree vlan vlan# [detail]
```

- 检验生成树配置

SwitchX#

```
debug spanning-tree pvst+
```

- 显示 PVST+ 事件调试消息

检验 PVRST+

```
SwitchX# show spanning-tree vlan 30
VLAN0030
Spanning tree enabled protocol rstp
Root ID Priority 24606
Address 00d0.047b.2800
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 24606 (priority 24576 sys-id-ext 30)
Address 00d0.047b.2800
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
Interface Role Sts Cost Prio.Nbr  Type
-------- ----- --- ---  --------  ----
Gi1/1     Desg FWD  4    128.1     P2p
Gi1/2     Desg FWD  4    128.2     P2p
Gi5/1     Desg FWD  4    128.257   P2p
```

将生成树模式设置为 PVRST+。

配置根桥和次根桥

VLAN 1 的根
1 Gb/s
VLAN 2 的根
分布层
分布层
交换机 A
交换机 B
100 Mb/s
VLAN 1 的转发端口
VLAN 2 的阻塞端口
VLAN 2 的转发端口
VLAN 1 的阻塞端口
327P_139
接入层

配置根桥和次根桥：SwitchA

```
SwitchA(config)#
spanning-tree vlan 1 root primary
```

- 此命令强制交换机成为 VLAN 1 的根桥。

```
SwitchA(config)#
spanning-tree vlan 2 root secondary
```

- 此命令强制交换机成为 VLAN 2 的次根桥。

或者

```
SwitchA(config)#
spanning-tree vlan # priority priority
```

- 此命令可静态配置优先级（增量为 4096）。

配置根桥和次根桥：SwitchB

```
SwitchB(config)#
spanning-tree vlan 2 root primary
```

- 此命令强制交换机成为 VLAN 2 的根桥。

```
SwitchB(config)#
spanning-tree vlan 1 root secondary
```

- 此命令强制交换机成为 VLAN 1 的次根桥。

或者

```
SwitchB(config)#
spanning-tree vlan # priority priority
```

- 此命令可静态配置优先级（增量为 4096）。

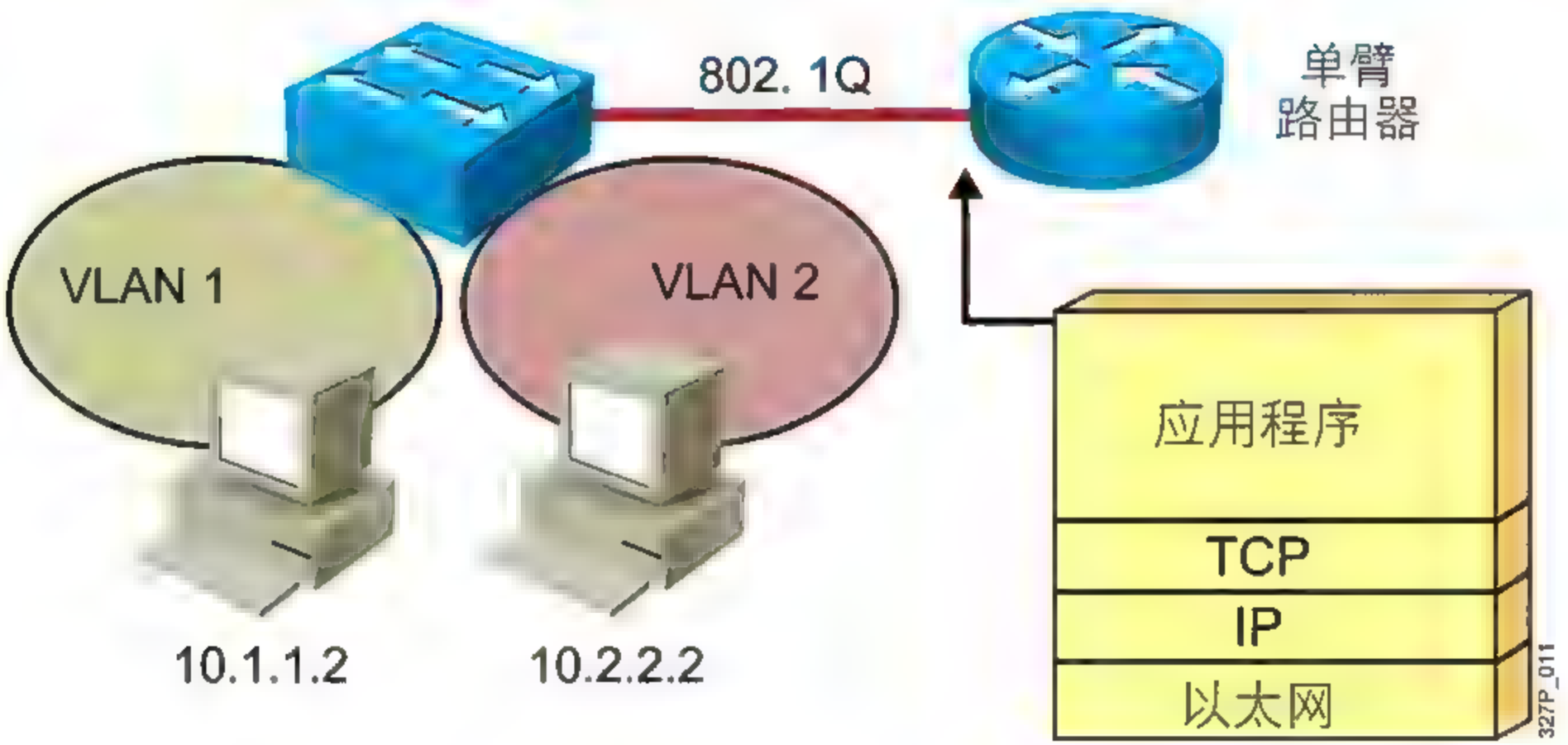
总结

- 冗余交换拓扑包括多宿主交换和 EtherChannel。
- 冗余交换拓扑会导致环路问题，例如广播风暴。
- 802.1D STP 可建立无环路的网络。
- 最初的 STP 已通过 PVST+ 和 RSTP 得以增强。

VLAN 间路由

中型交换网络结构

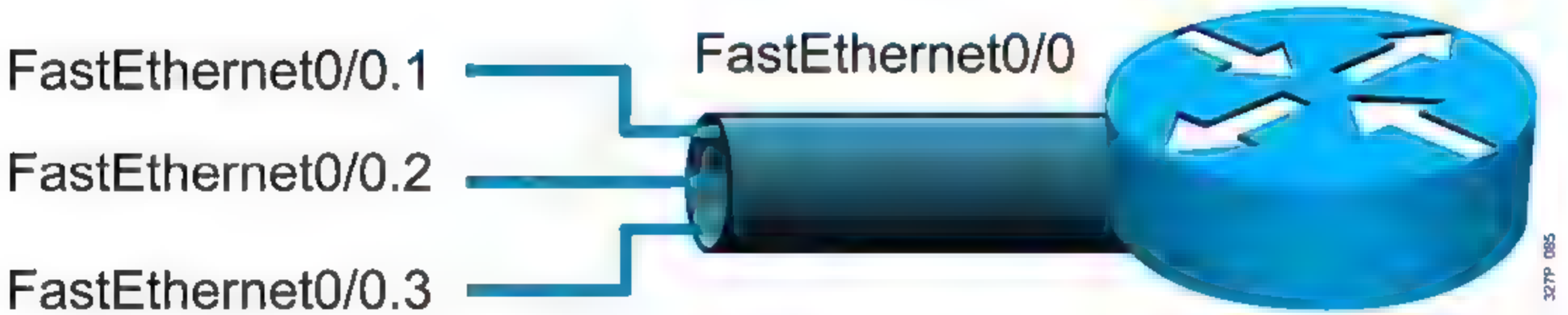
VLAN 到 VLAN 的概述



- 网络层设备将多个广播域融为一体。

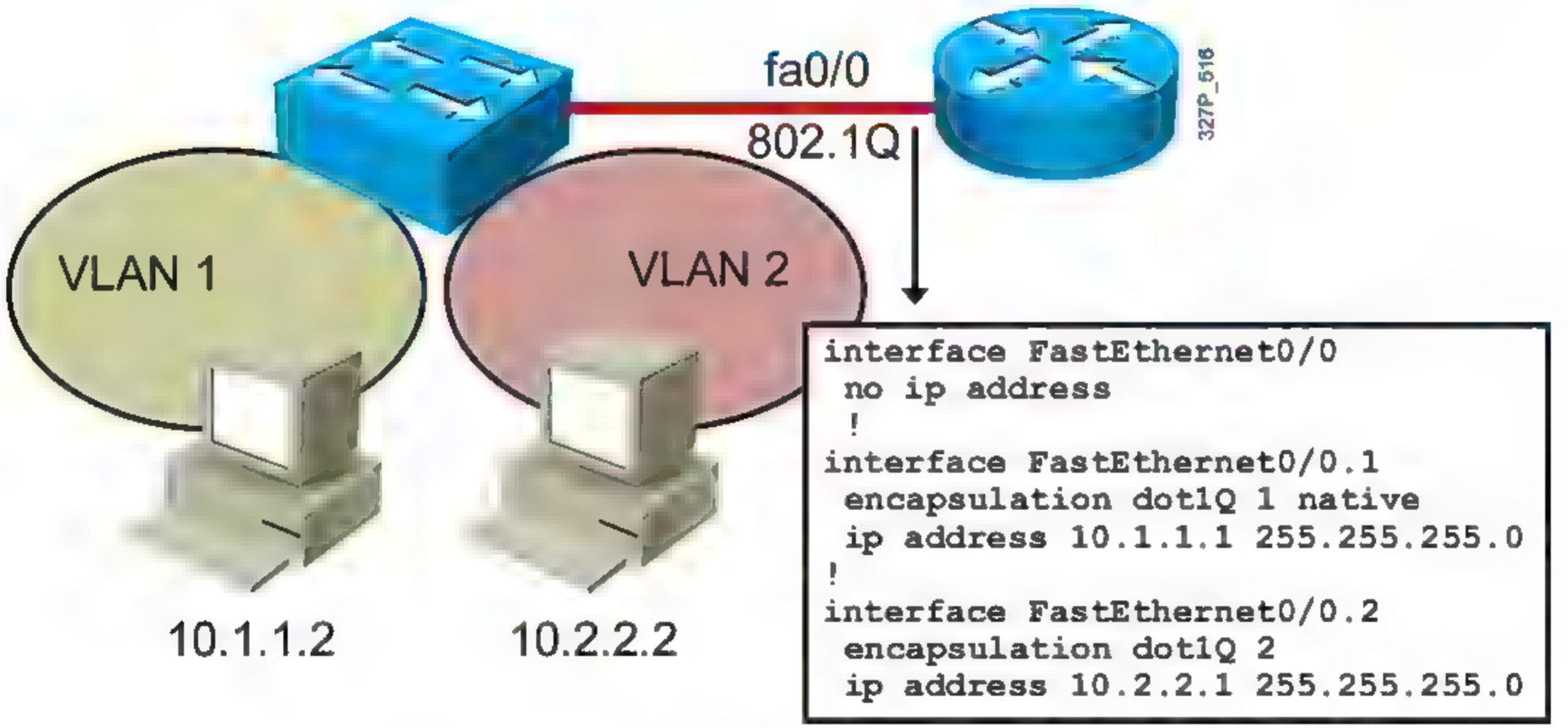
Systems Inc. 保留所有权利。

将物理接口划分为子接口



- 物理接口可划分为多个子接口。

使用 802.1Q 中继路由



© 2008 Cisco Systems, Inc. 保留一切权利

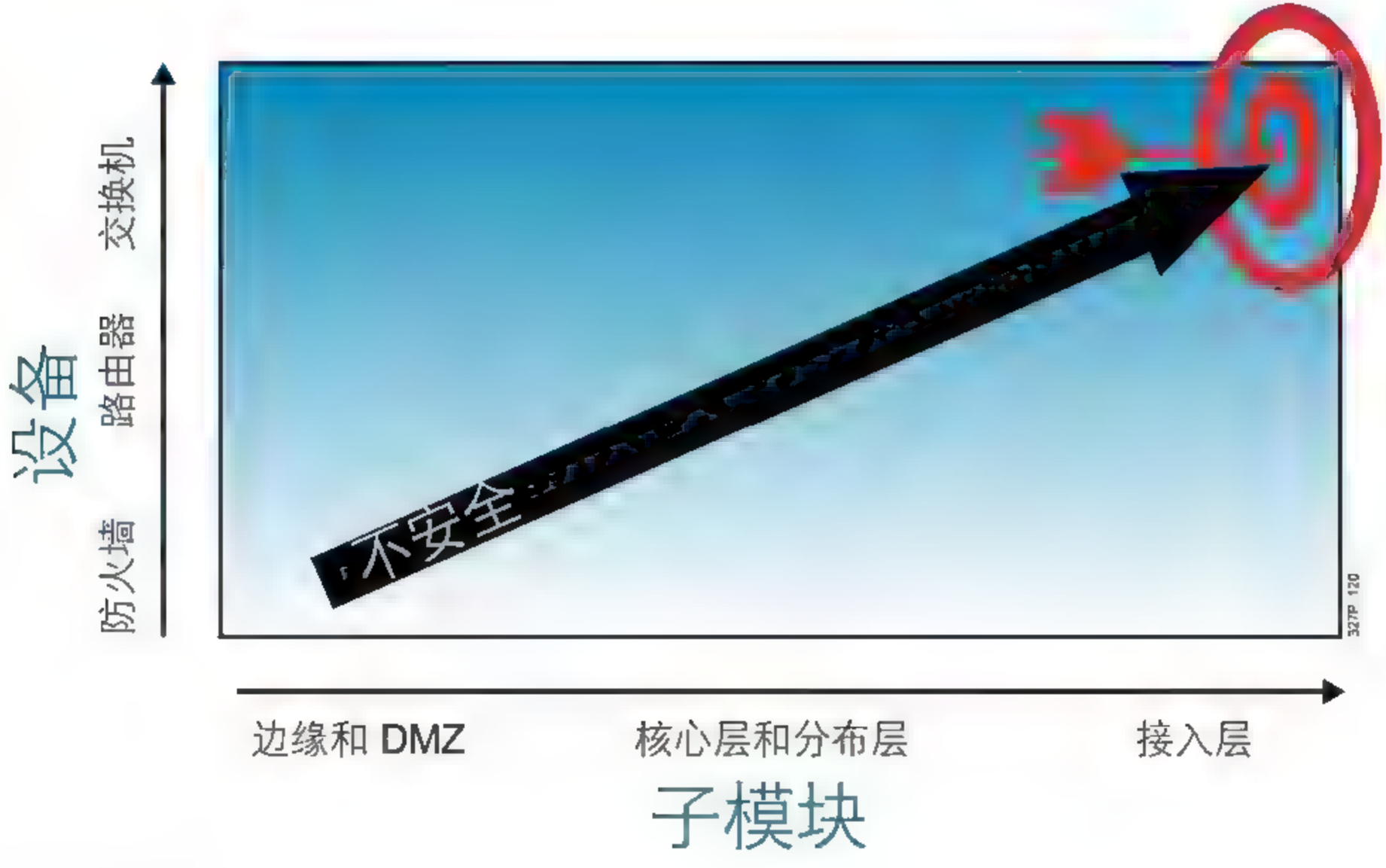
总结

- 使用单臂路由器的 VLAN 路由利用外部路由器在 VLAN 间传输流量。
- 单臂路由器为每个 VLAN 和 802.1Q 中继封装配置了子接口。

保护可扩展网络

中型交换网络结构

交换机安全概述



建议做法：新交换机设备

- 考虑或建立有组织的安全策略。
- 保证交换机设备的安全 ：
  - 安全访问交换机。
  - 保证交换机协议的安全 。
  - 降低交换机带来的风险。

建议做法：交换机安全

- 安全访问交换机：
  - 设置系统口令。
  - 保证对控制台的物理访问安全 。
  - 保证通过 Telnet 进行的访问安全 。
  - 如果可能，使用 SSH。
  - 禁用 HTTP。
  - 配置系统警告标语。
  - 禁用不需要的服务。
  - 如果 syslog 可用，就使用它 。

建议做法：交换机安全（续）

- 保证交换机协议的安全 ：
  - 修改 Cisco 发现协议，并且仅在需要时使用。
  - 保护生成树。
- 降低交换机带来的风险：
  - 对中继链路采取预防措施。
  - 尽可能减少物理端口的访问。
  - 为未使用和已使用的端口建立标准访问端口配置。

端口安全

利用 MAC 地址限制端口访问来确保端口安全。

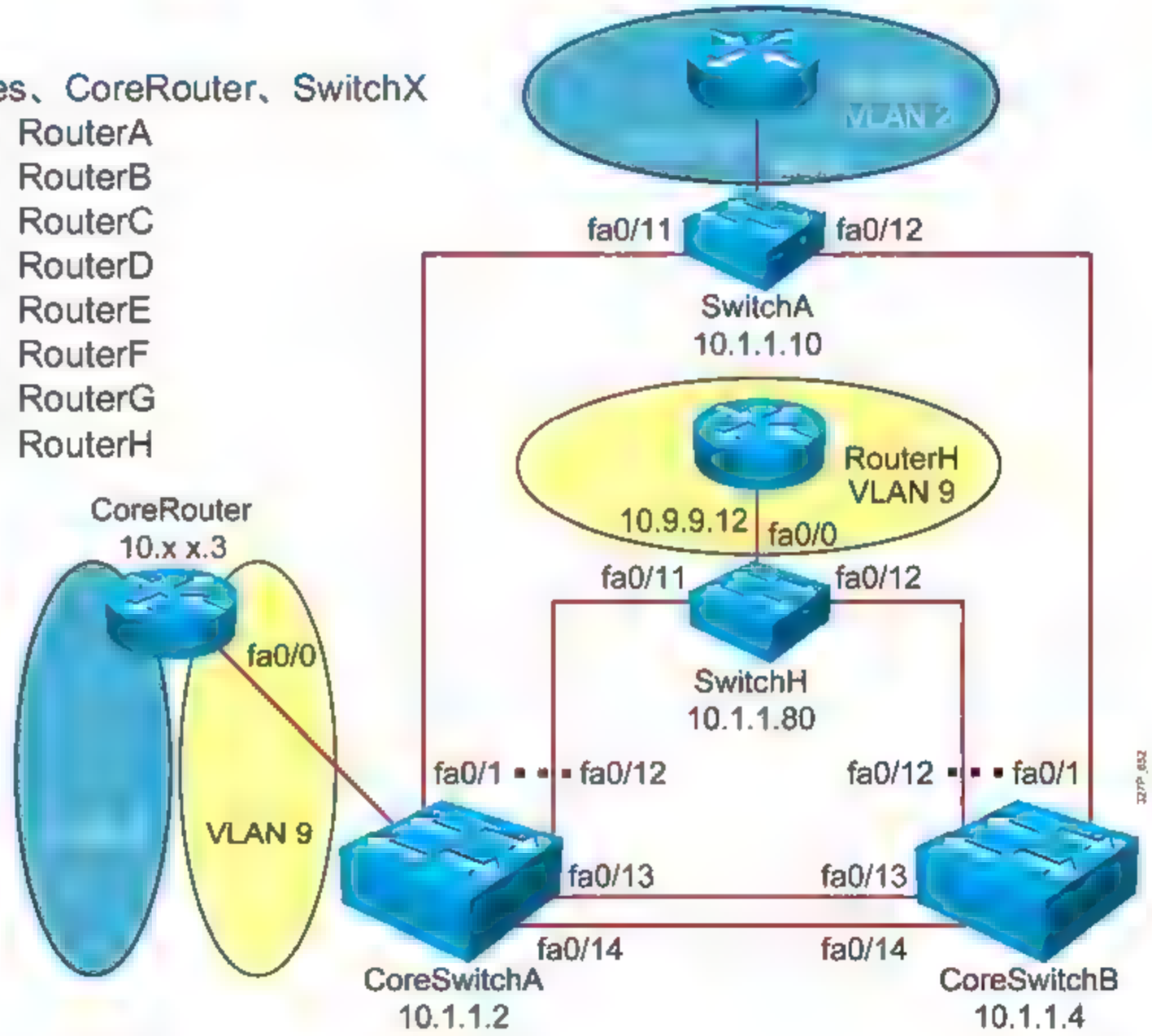
基于 802.1X 端口的身份验证

通过交换机访问网络时，需要进行身份验证。

© 2008 Cisco Systems, Inc. 保留所有权利。

可视目标 2-1：配置可扩展交换网络

子网	VLAN	设备
10.1.1.0	1	Core Switches、CoreRouter、SwitchX
10.2.2.0	2	CoreRouter、RouterA
10.3.3.0	3	CoreRouter、RouterB
10.4.4.0	4	CoreRouter、RouterC
10.5.5.0	5	CoreRouter、RouterD
10.6.6.0	6	CoreRouter、RouterE
10.7.7.0	7	CoreRouter、RouterF
10.8.8.0	8	CoreRouter、RouterG
10.9.9.0	9	CoreRouter、RouterH



© 2008 Cisco Systems, Inc. 保留所有权利。

总结

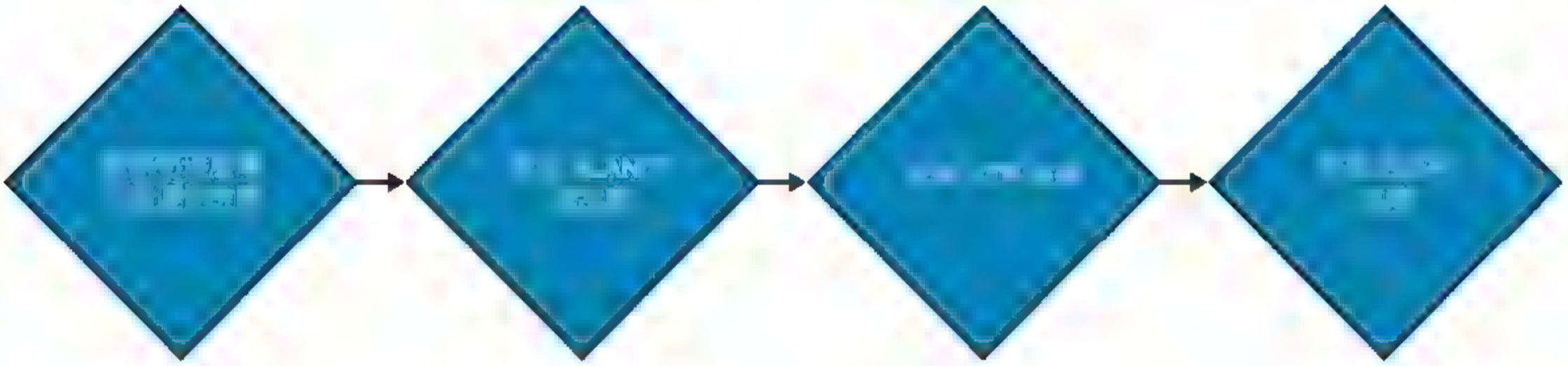
- 遵循建议做法，通过使用口令、取消激活未使用的端口、配置身份验证和使用端口安全来保证交换拓扑的安全。
- 要保证交换机设备的安全 ，您必须对交换机的访问和交换机所使用的协议进行安全保护。

CISCO

交换网络故障排除

中型交换网络结构

交换机故障排除

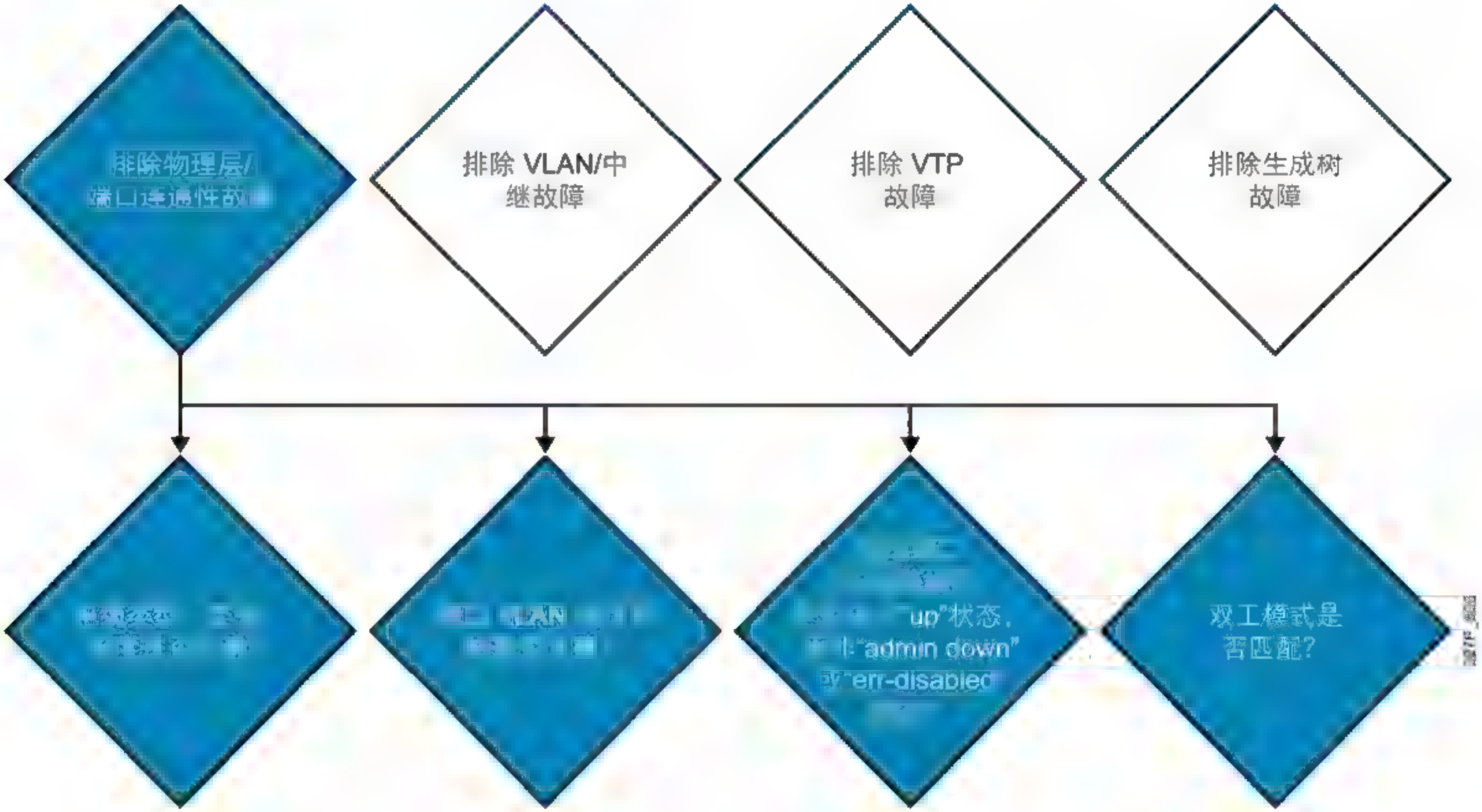


故障排除的通用建议：

- 熟悉常规交换机操作。
- 拥有准确的网络物理图和逻辑图。
- 制定计划。
- 未检验某个组件确实在工作之前，请勿假设其正在工作。

© 2008 Cisco Systems, Inc. 保留所有权利。

端口连通性故障排除

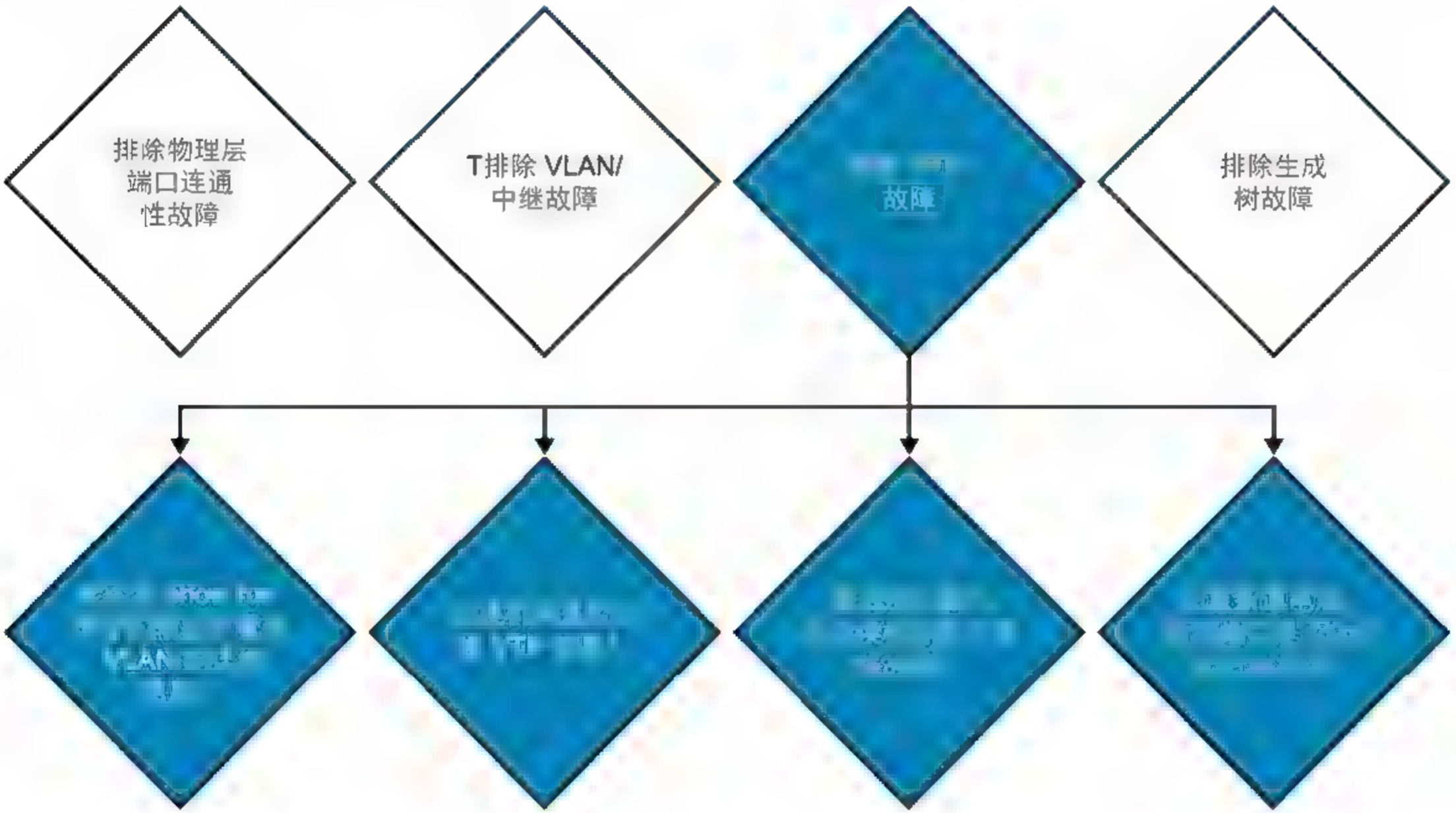


© 2008 Cisco Systems, Inc. 保留所有权利。

VLAN 和中继故障排除

© 2008 Cisco Systems, Inc. 保留所有权利。

VTP 故障排除



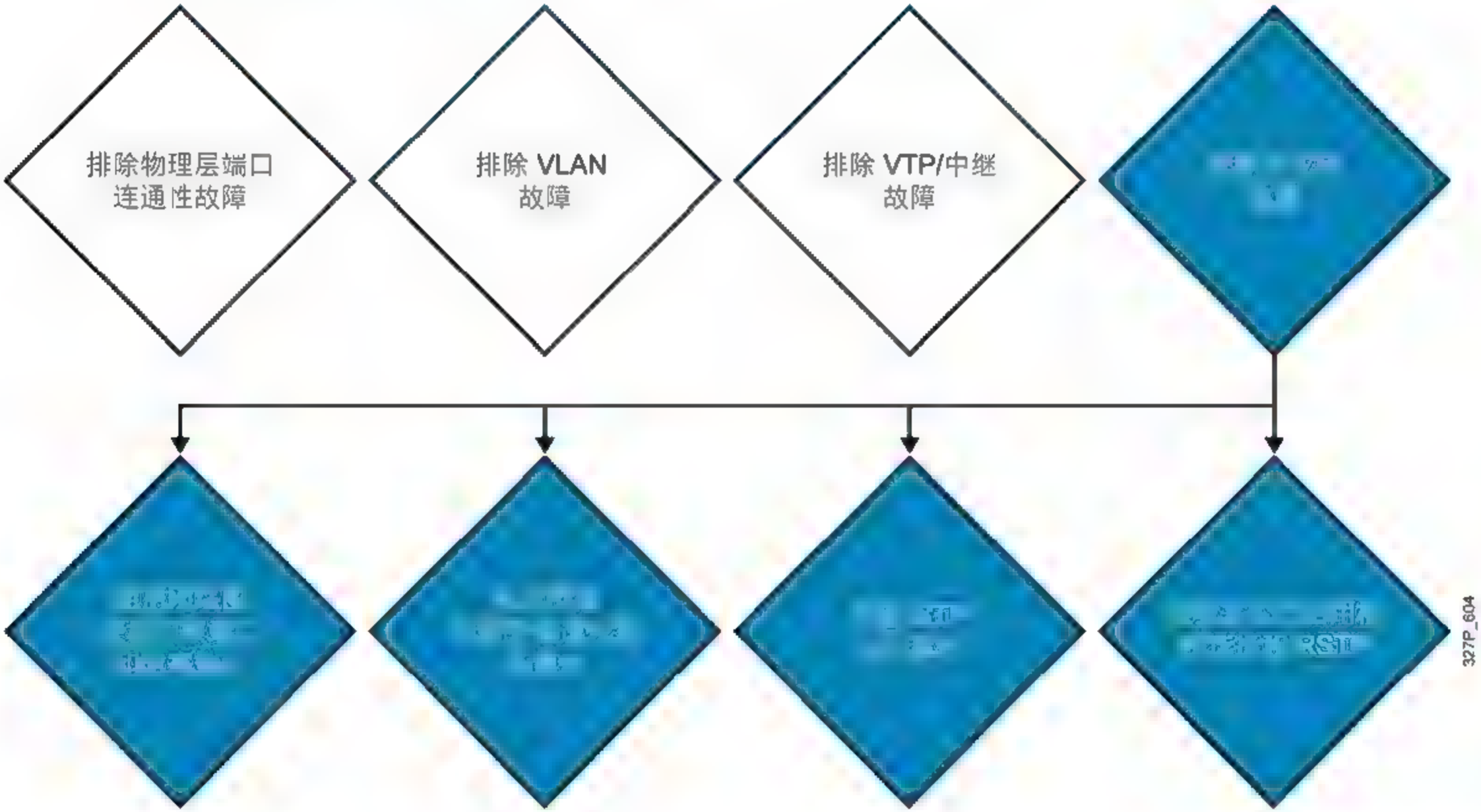
© 2008 Cisco Systems, Inc. 保留所有权利。

VTP 排除故障（续）

如果 Catalyst 交换机不能交换 VTP 信息，请检验以下设置：

- 互连交换机的所有端口是否都已配置为中继。
- 所有服务器交换机中的 VLAN 都处于活动状态。
- 至少有一台 VTP 服务器交换机。
- 如果分配了 VTP 域名和口令，所有交换机上的 VTP 域名和口令都要匹配（区分大小写）。
- 所有交换机都运行相同版本的 VTP。
- 检验处于透明模式的交换机的域名和 VTP 版本。
- 注意扩展范围内的 VLAN 不能传播 VTPv1 和 VTPv2。

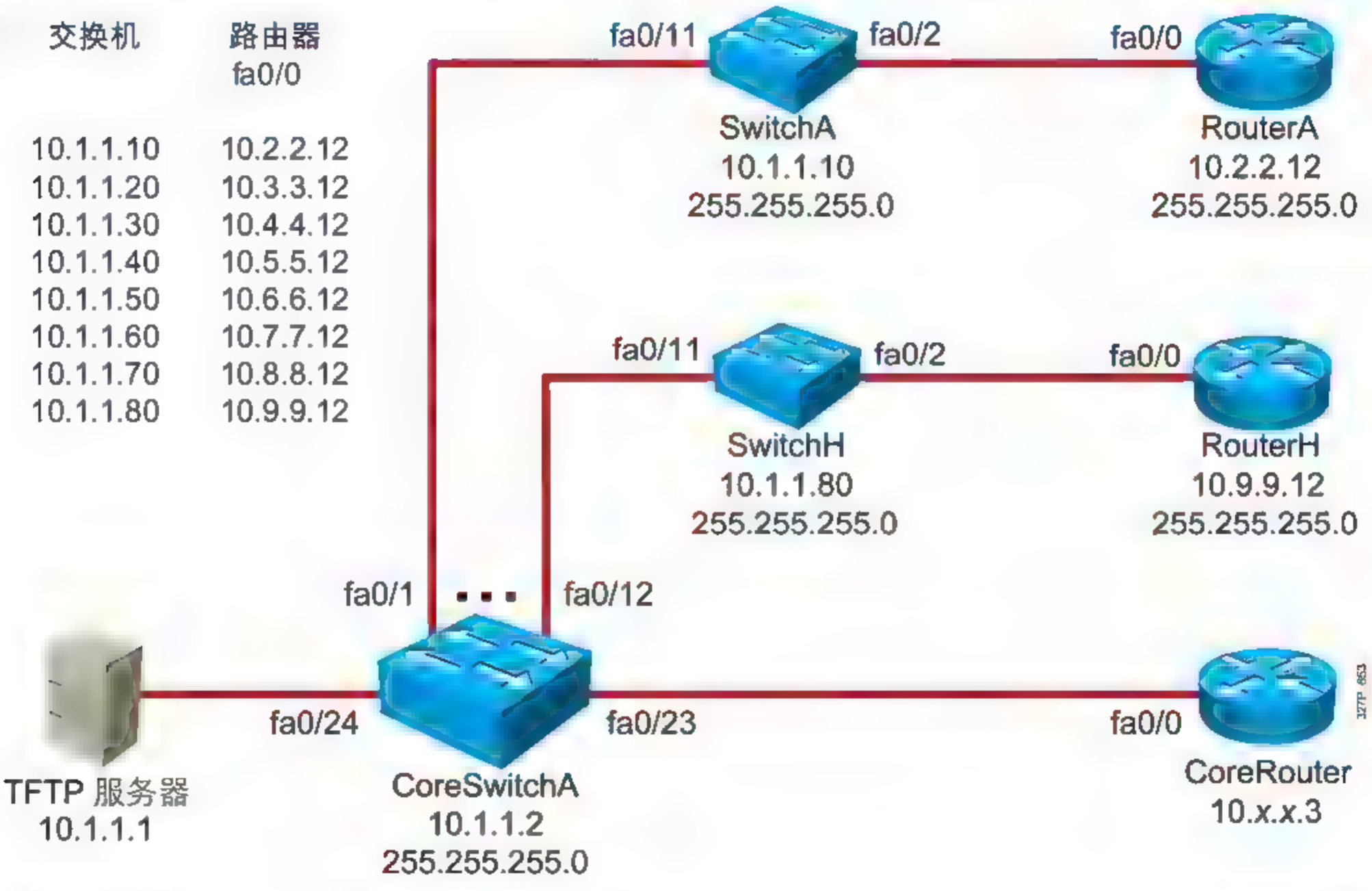
生成树故障排除



© 2008 Cisco Systems, Inc. 保留所有权利。

可视目标 2-2：交换网络故障排除

工作组	交换机	路由器 fa0/0
A	10.1.1.10	10.2.2.12
B	10.1.1.20	10.3.3.12
C	10.1.1.30	10.4.4.12
D	10.1.1.40	10.5.5.12
E	10.1.1.50	10.6.6.12
F	10.1.1.60	10.7.7.12
G	10.1.1.70	10.8.8.12
H	10.1.1.80	10.9.9.12



总结

- 了解网络正常工作的前提条件是有效排除交换网络故障的前提。
- 硬件问题和端口配置错误都会导致端口连通方面的问题。
- 本地 VLAN 不匹配和中继模式不匹配会阻碍建立中继链路。
- 对 VTP 进行故障排除时，了解 VTP 的工作方式是最佳的防御措施。
- 处理 STP 故障的主要目标之一是断开环路并尽快恢复连通。

CISCO

单元总结

- 扩展公司网络时，VLAN、VTP 和中继可提供一个可分段、灵活和安全的交换网络基础设施。
- STP 及其后继 RSTP 可解决冗余交换网络固有的桥接环路问题。
- VLAN 间进行路由的一种方法是使用子接口和 802.1Q 中继配置“单臂路由器”。
- 排除交换网络的故障需要了解底层协议（如 VTP、PVRST+ 和 802.1Q）的特征。

检查路由操作

中型路由网络结构

静态路由与动态路由

静态路由

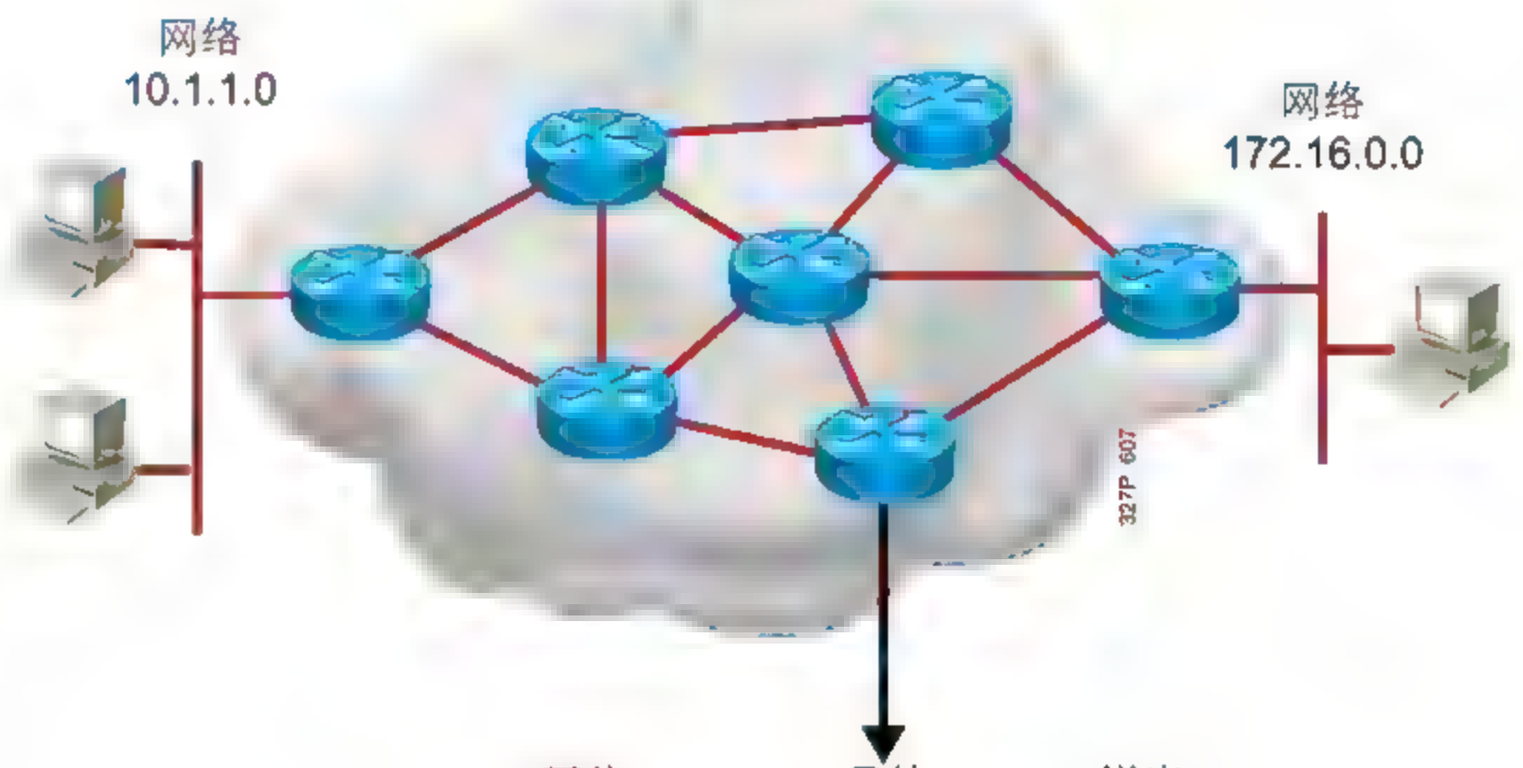
- 这种路由由网络管理员手动输入路由器命令管理

动态路由

- 这种路由由网络路由协议根据拓扑或流量改变而自动调整

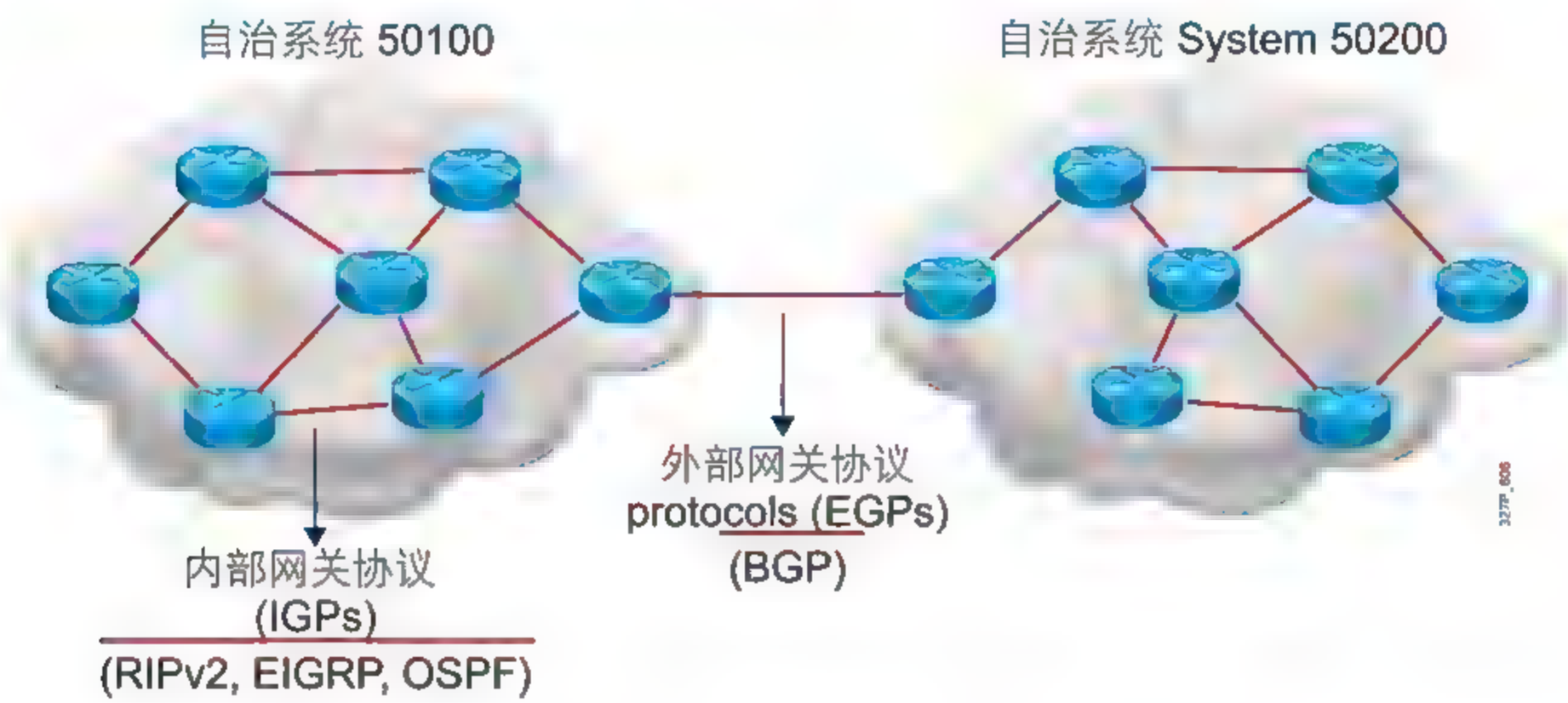
什么是动态路由协议？

- 路由器之间使用路由协议确定到达远程网络的路径，并在路由表中维护这些网络。
- 确定路径后，路由器可以将路由协议路由到已获知的网络。



网络协议	目的网络	送出接口
EIGRP	10.1.1.0	FA0/1
OSPF	172.16.0.0	FA0/2

自治系统：内部路由协议和外部路由协议

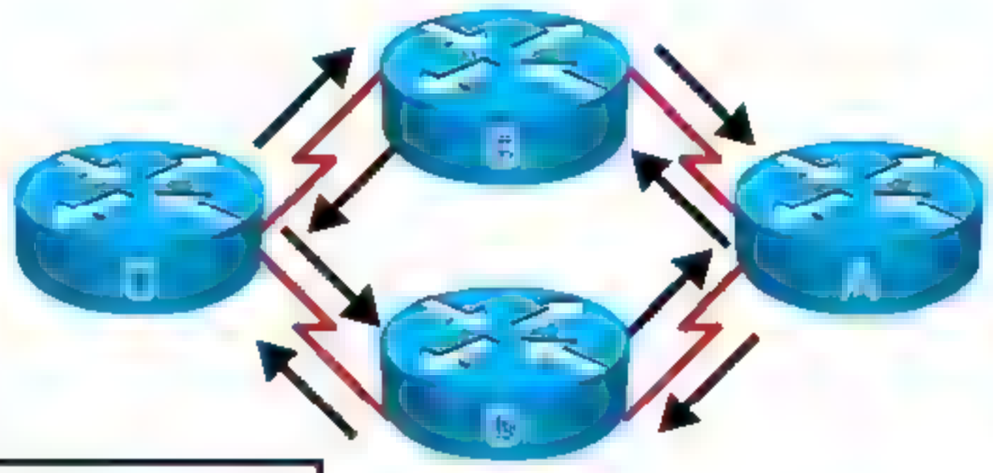


- 自治系统是通用管理域中的网络的集合。
- 内部网关协议在自治系统中工作。
- 外部网关协议连接不同的自治系统。

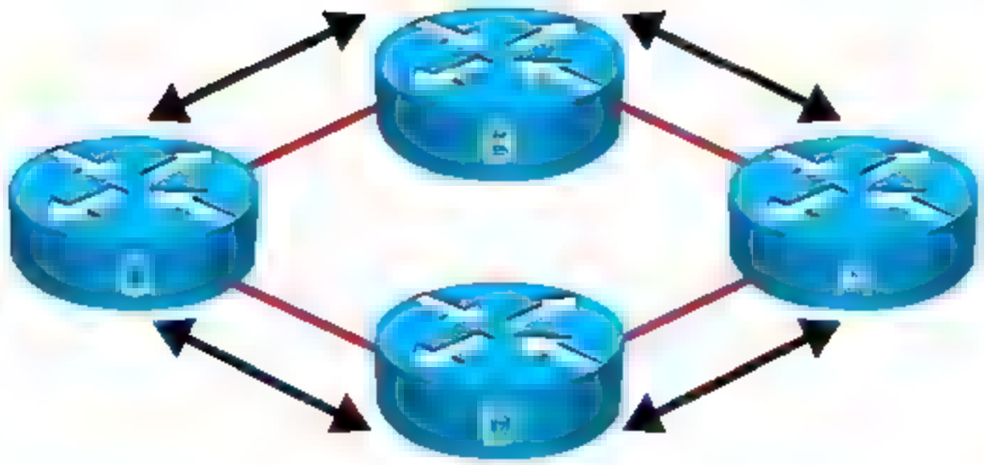
© 2008 Cisco Systems, Inc. 保留所有权利。

路由协议的类型

距离矢量



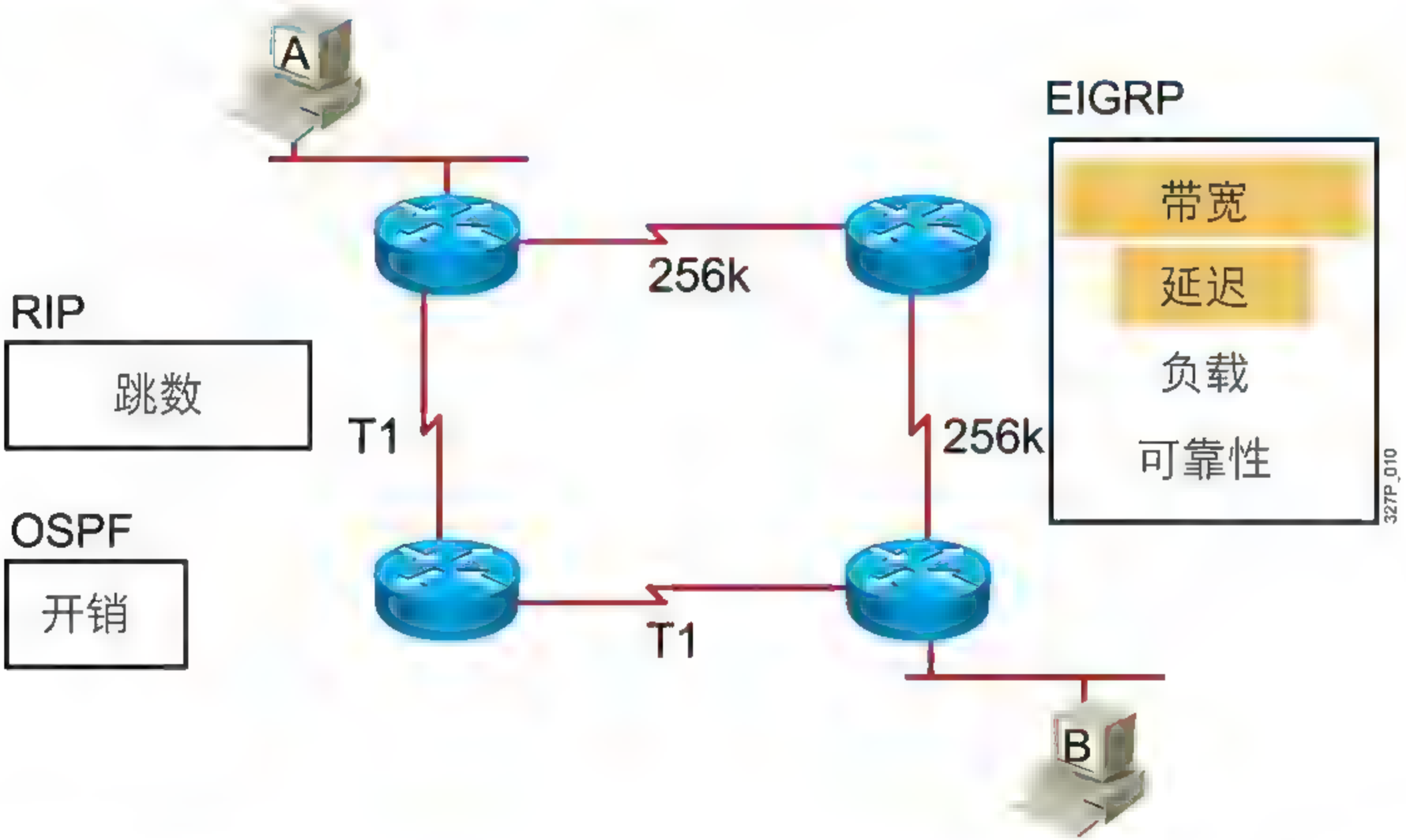
高级距离矢量



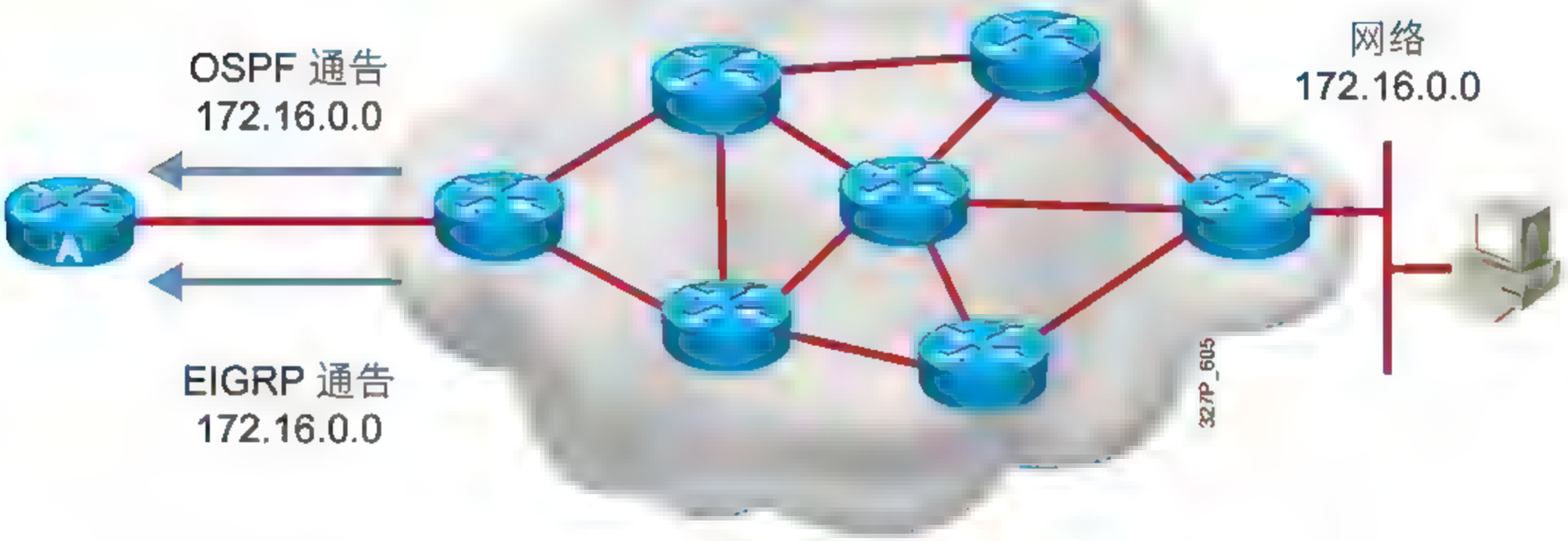
链路状态

327P 086

使用度量选择最佳路由



管理距离：评价路由来源

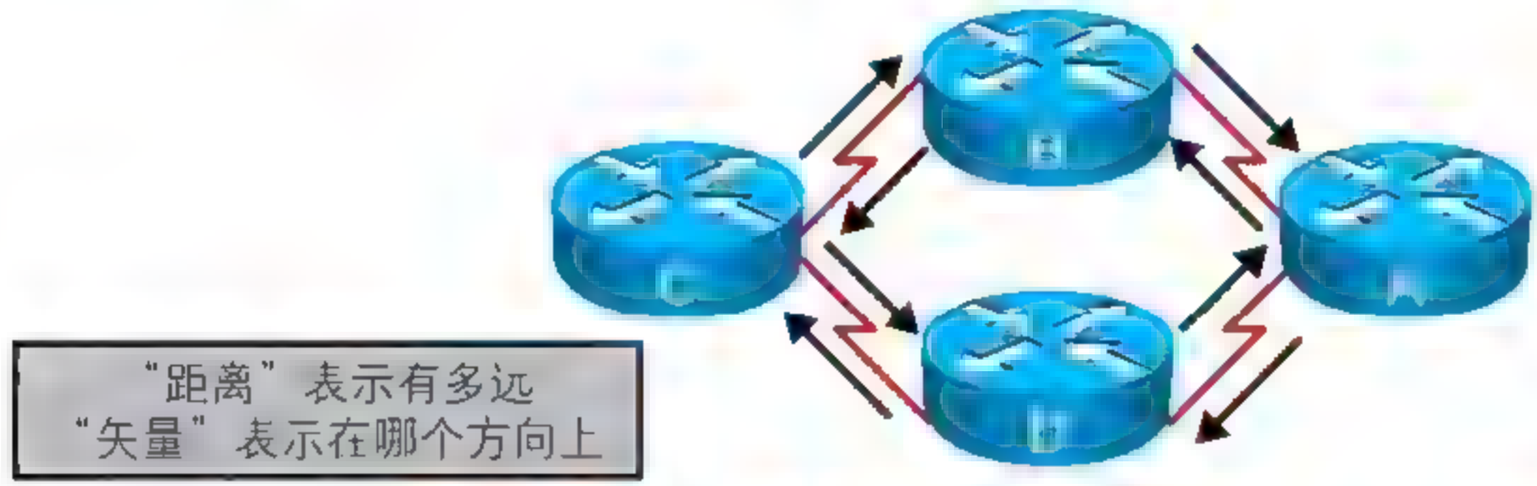


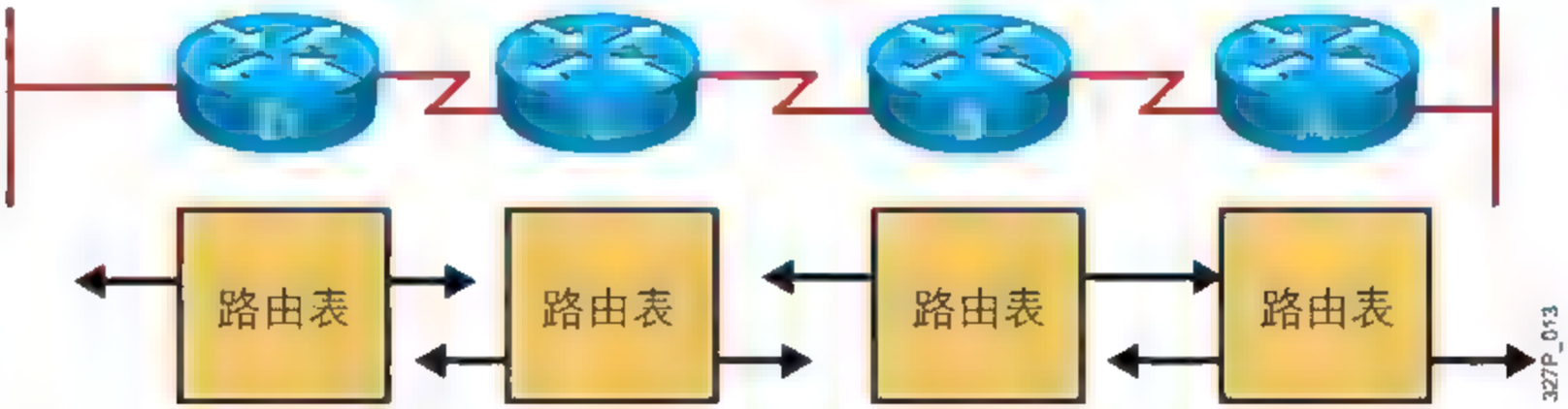
路由器使用最佳管理距离选择路由来源：

- OSPF 的管理距离是 110。
- EIGRP 的管理距离是 90。

© 2008 Cisco Systems, Inc. 保留所有权利。

距离矢量路由协议





路由器定期将路由表的副本传递给邻居路由器并累计距离矢量。

信息来源和发现路由

路由表		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

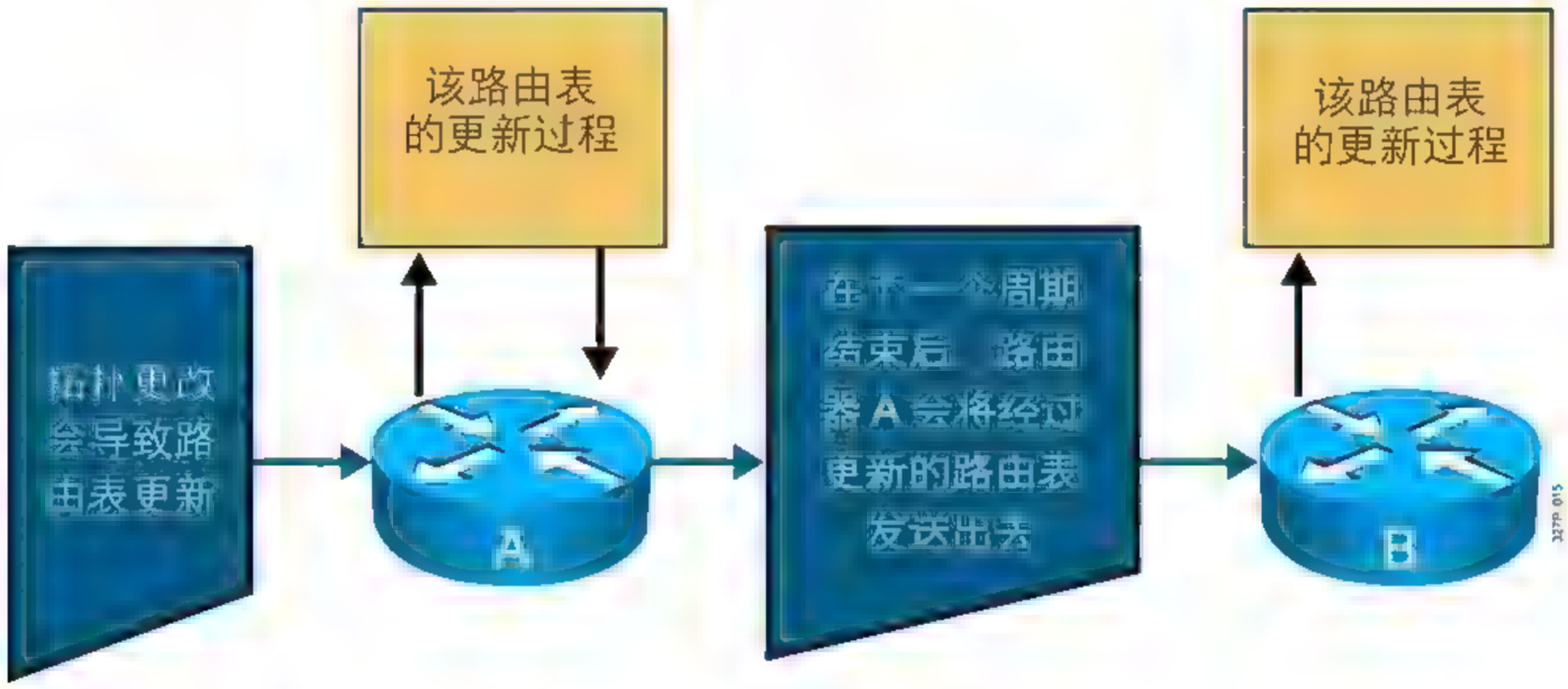
路由表		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

路由表		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

327P 014

路由器从每个邻居处发现到达目的地的最佳路径。

维护路由信息



从一台路由器到另一台路由器逐步进行更新。

不一致的路由条目：计数至无穷大和路由环路

路由表		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

路由表		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

路由表		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

327P_017

每个节点都会维护从自身到每个可能的目的网络的距离。

计数至无穷大

路由表		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

路由表		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

路由表		
10.3.0.0	S0	0
10.4.0.0	E0	已断开
10.2.0.0	S0	1
10.1.0.0	S0	2

327P 016

缓慢的收敛会产生不一致的路由。

计数至无穷大（续）

路由表		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

路由表		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

路由表		
10.3.0.0	S0	0
10.4.0.0	S0	2
10.2.0.0	S0	1
10.1.0.0	S0	2

327P_018

路由器 C 得出到达网络 10.4.0.0 的最佳路径是通过路由器 B。

计数至无穷大（续）

路由表		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	4

路由表		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	3
10.1.0.0	S0	1

路由表		
10.3.0.0	S0	0
10.4.0.0	S0	2
10.2.0.0	S0	1
10.1.0.0	S0	2

327P_019

路由器 A 更新其路由表以反映新的错误跳数。

计数至无穷大（续）

路由表		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	6

路由表		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	5
10.1.0.0	S0	1

路由表		
10.3.0.0	S0	0
10.4.0.0	S0	4
10.2.0.0	S0	1
10.1.0.0	S0	2

327P_020

网络 10.4.0.0 的跳数计数至无穷大。

计数至无穷大的解决方案：定义最大值

路由表		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	16

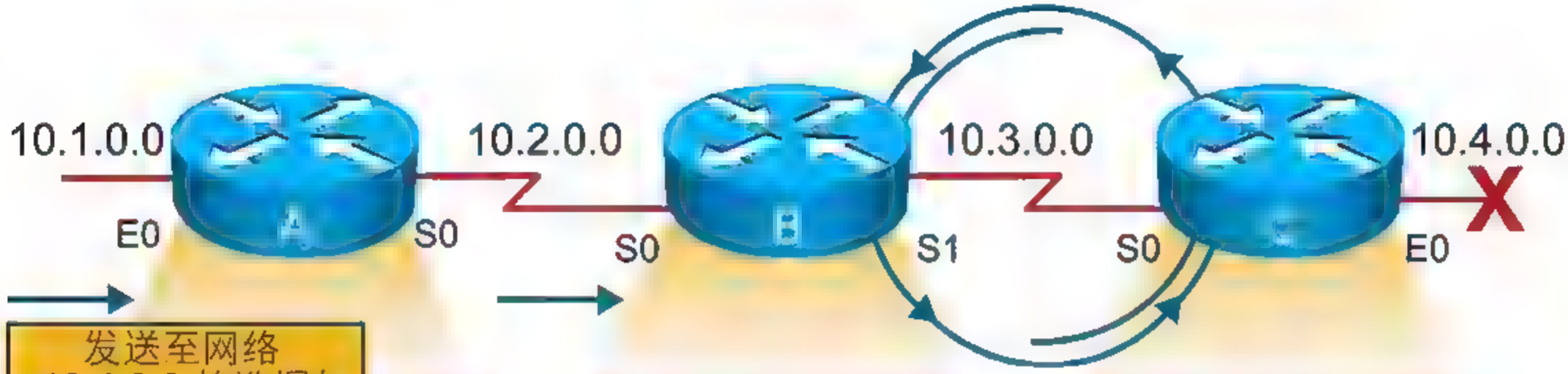
路由表		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	16
10.1.0.0	S0	1

路由表		
10.3.0.0	S0	0
10.4.0.0	S0	16
10.2.0.0	S0	1
10.1.0.0	S0	2

327P_021

设置跳数限制以防止无限环路。

路由环路



路由表		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	4

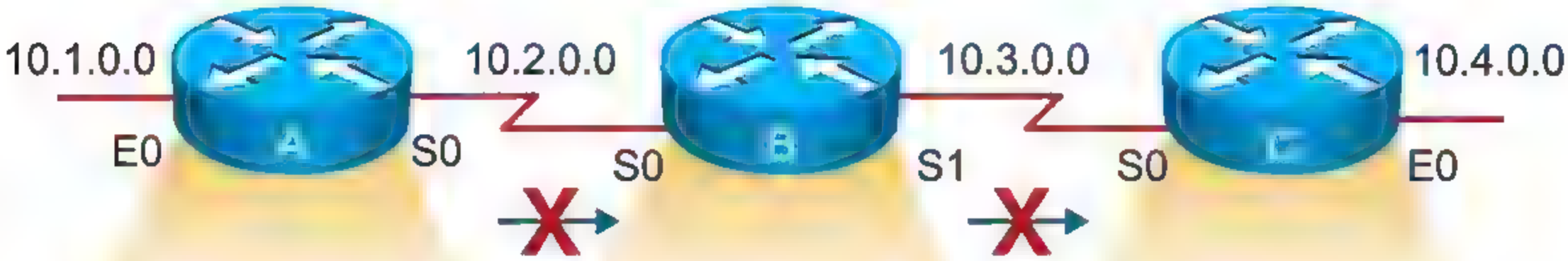
路由表		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	3
10.1.0.0	S0	1

路由表		
10.3.0.0	S0	0
10.4.0.0	S0	2
10.2.0.0	S0	1
10.1.0.0	S0	2

327P_022

前往网络 10.4.0.0 的数据包在路由器 B 和 C 之间来回传递（环路）

路由环路的解决方案：水平分割



路由表		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

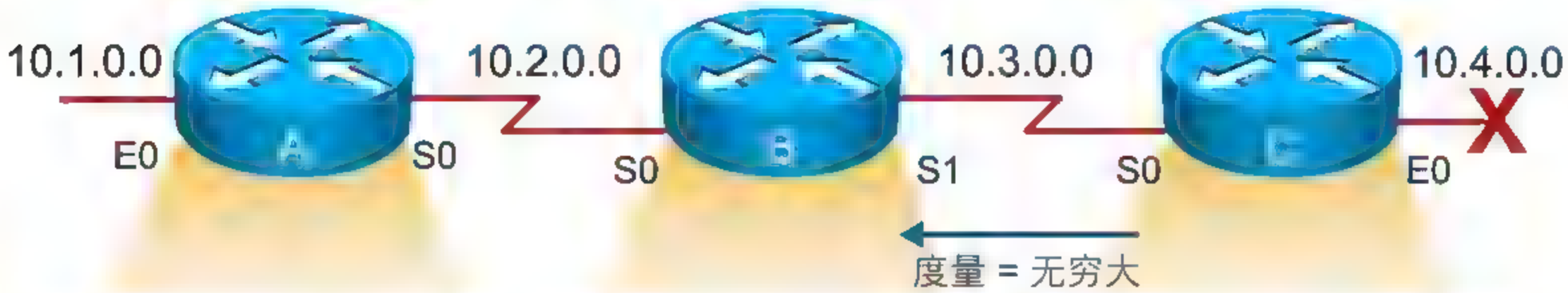
路由表		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

路由表		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

327P_023

向原始信息的来源方向返回路由信息毫无用处。

路由环路的解决方案：路由毒化和毒性反转



路由表		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

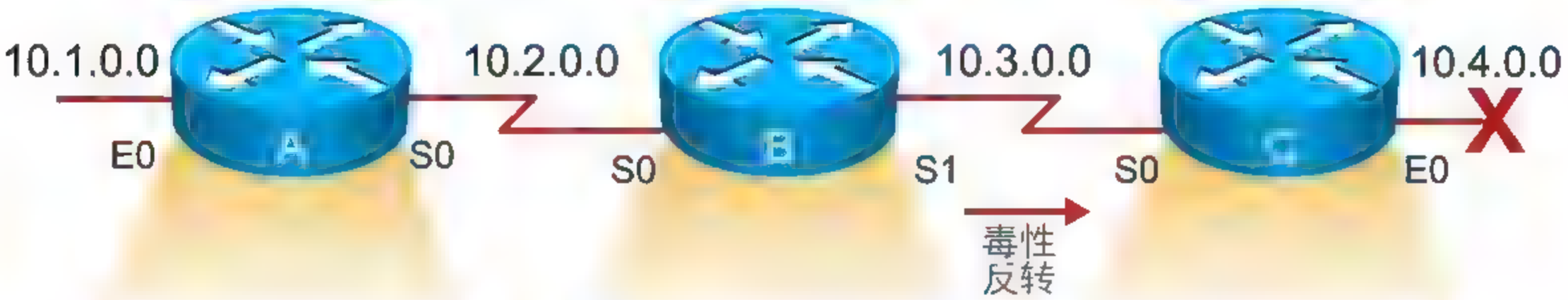
路由表		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

路由表		
10.3.0.0	S0	0
10.4.0.0	E0	已断开
10.2.0.0	S0	1
10.1.0.0	S0	2

327P_024

路由器将已经断开的路由的距离通告为无穷大。

路由环路的解决方案：
路由毒化和毒性反转（续）



路由表		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

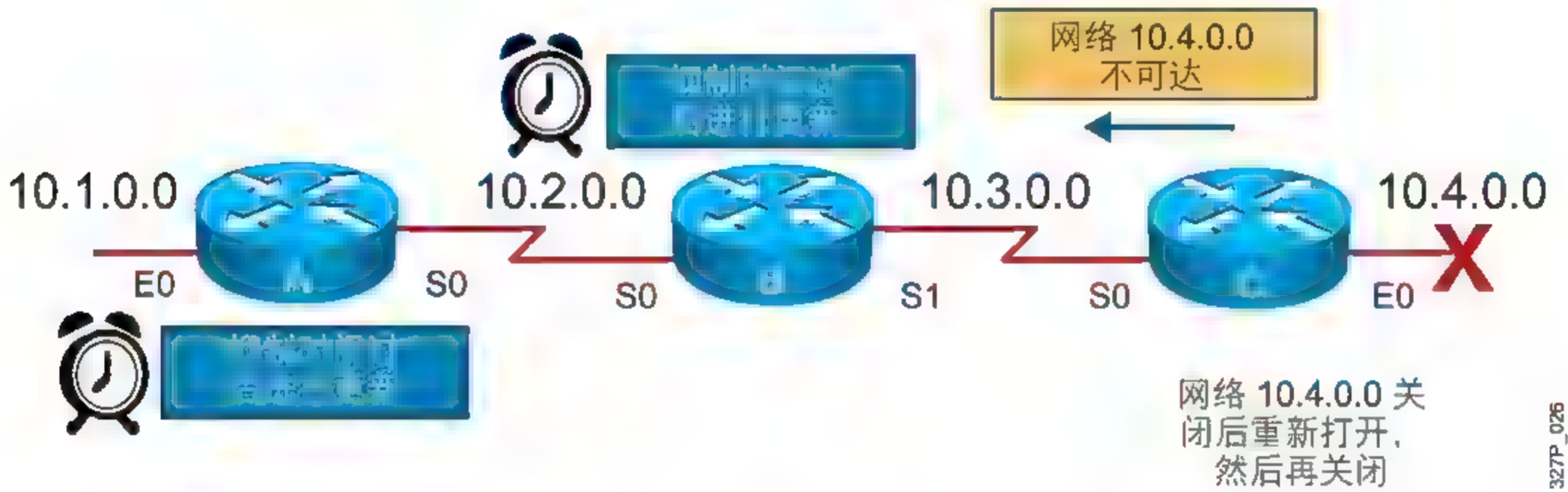
路由表		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	可能已断开
10.1.0.0	S0	1

路由表		
10.3.0.0	S0	0
10.4.0.0	S0	无穷大
10.2.0.0	S0	1
10.1.0.0	S0	2

327P_025

毒性反转会忽略水平分割。

路由环路的解决方案：抑制计时器

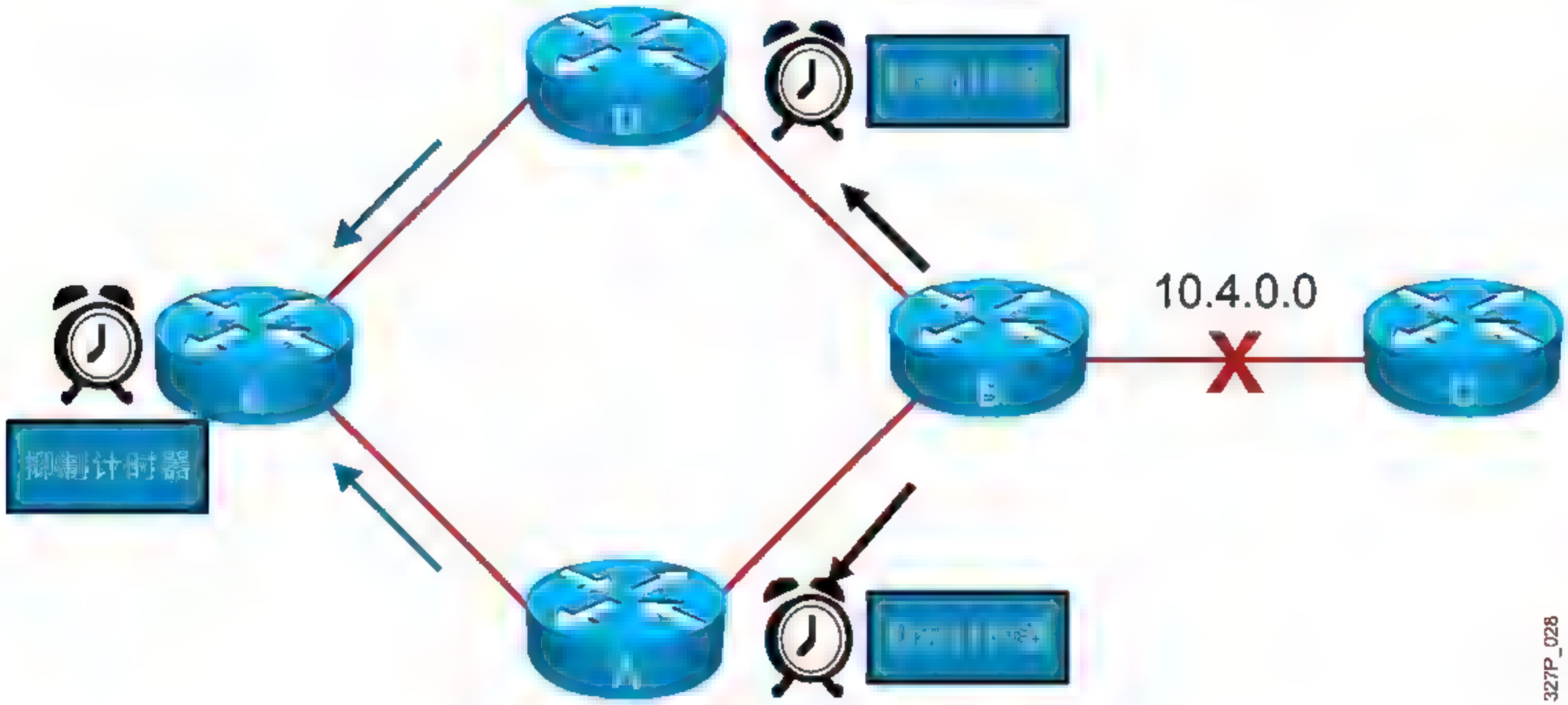


路由器为网络中的“可能有故障”状态保留条目，以便为其它路由器重新计算拓扑更改留出时间。

触发更新

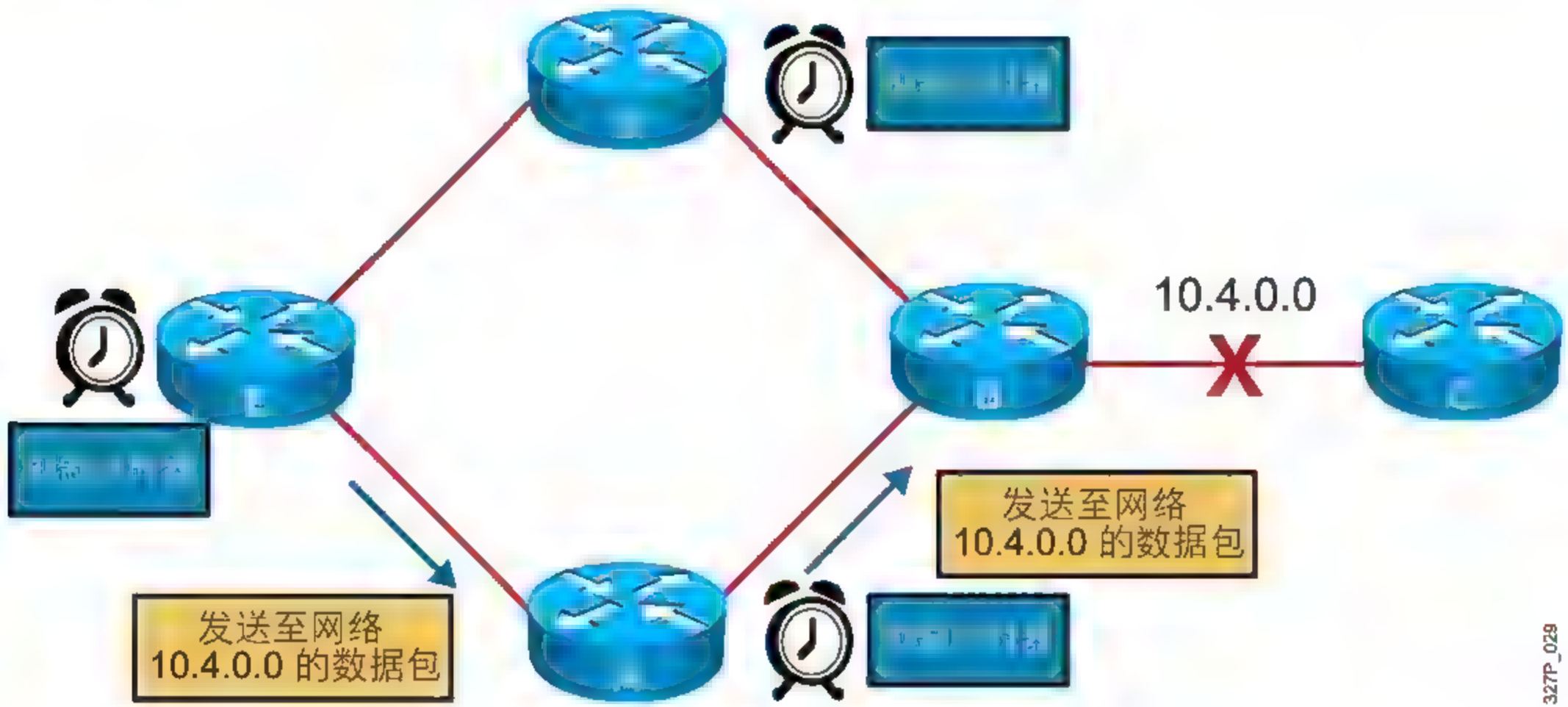
路由表发生变化时，路由器发送更新。

消除路由环路

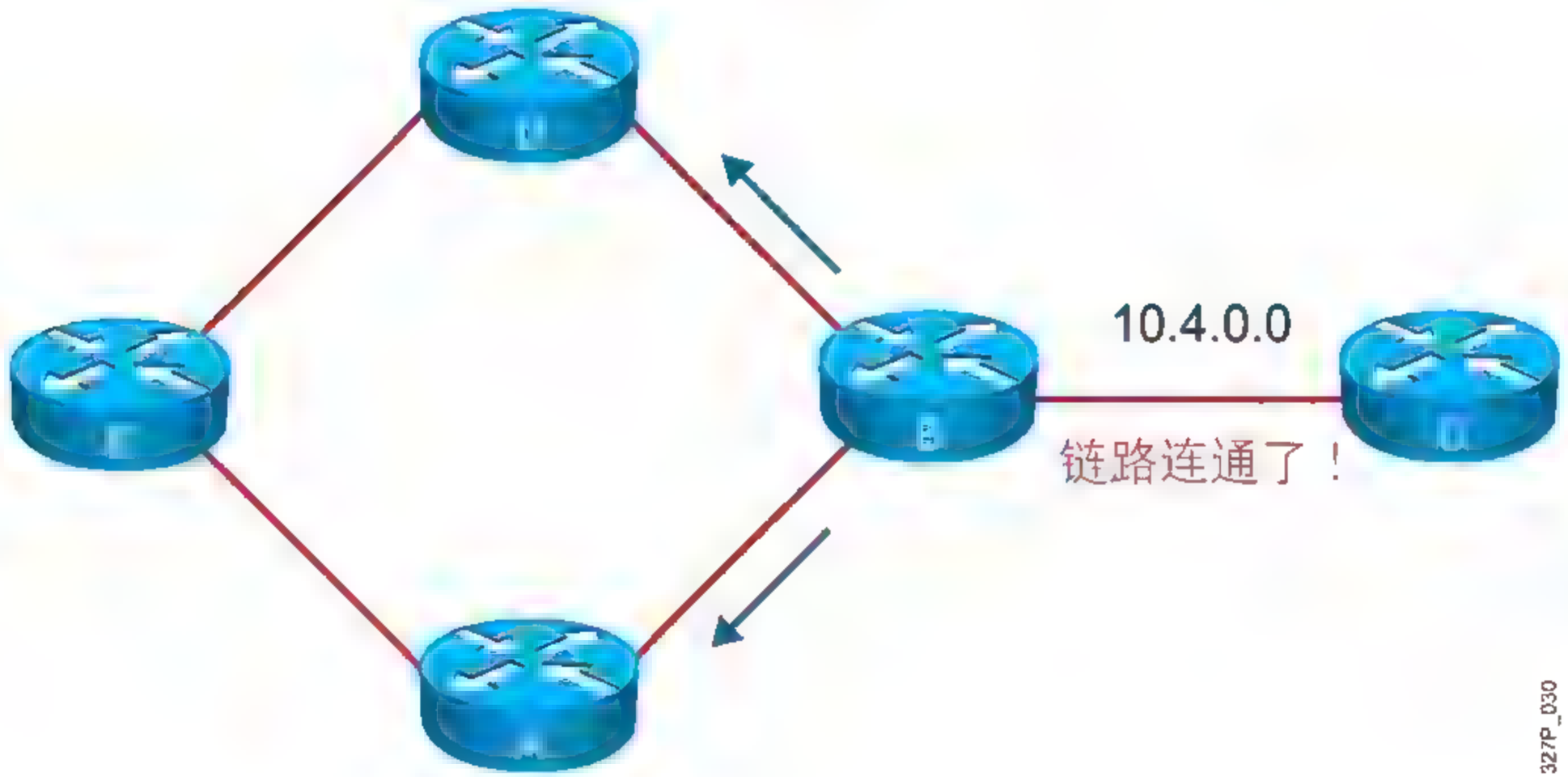


© 2008 Cisco Systems, Inc. 保留所有权利。

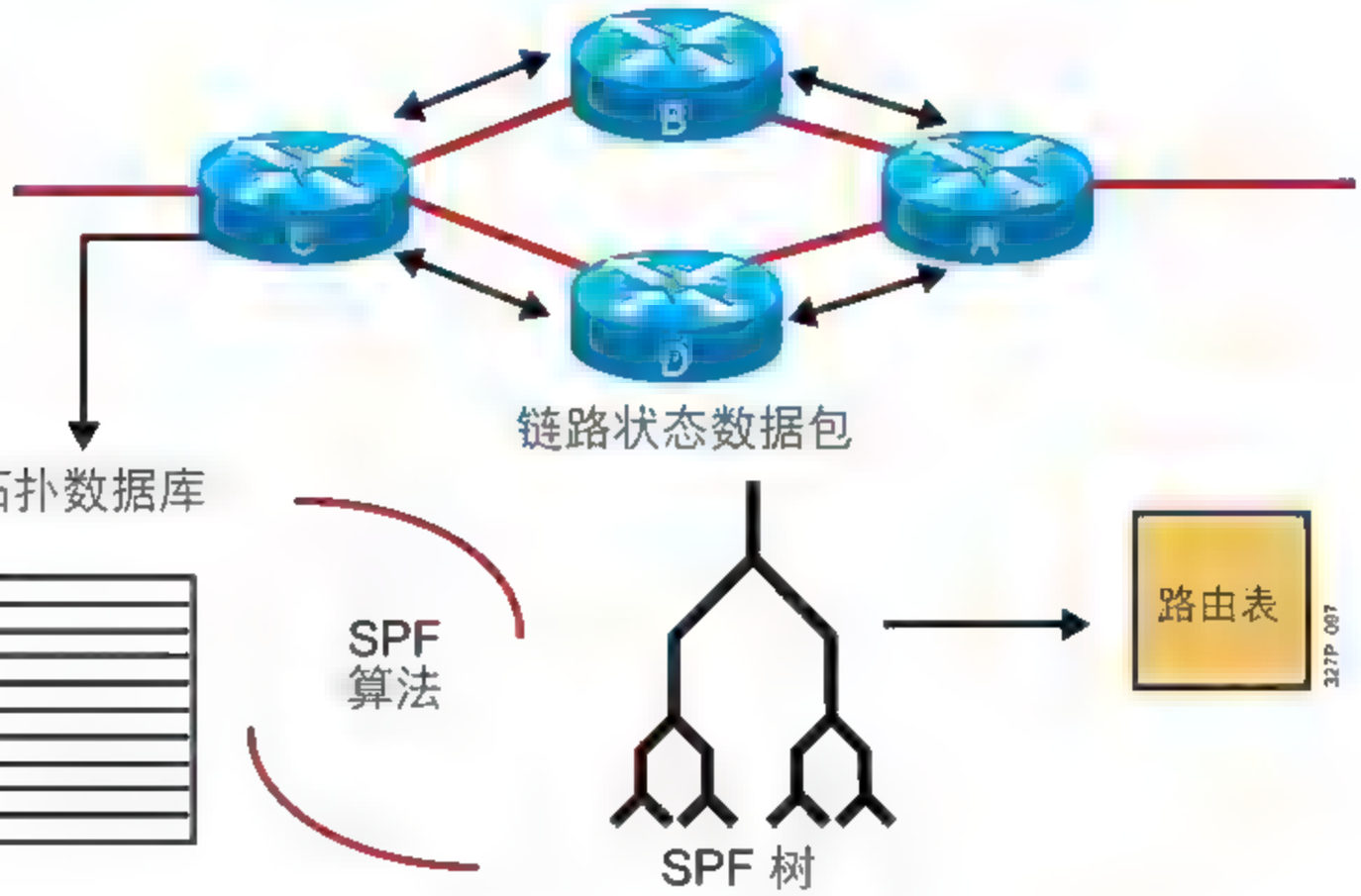
消除路由环路（续）



消除路由环路（续）



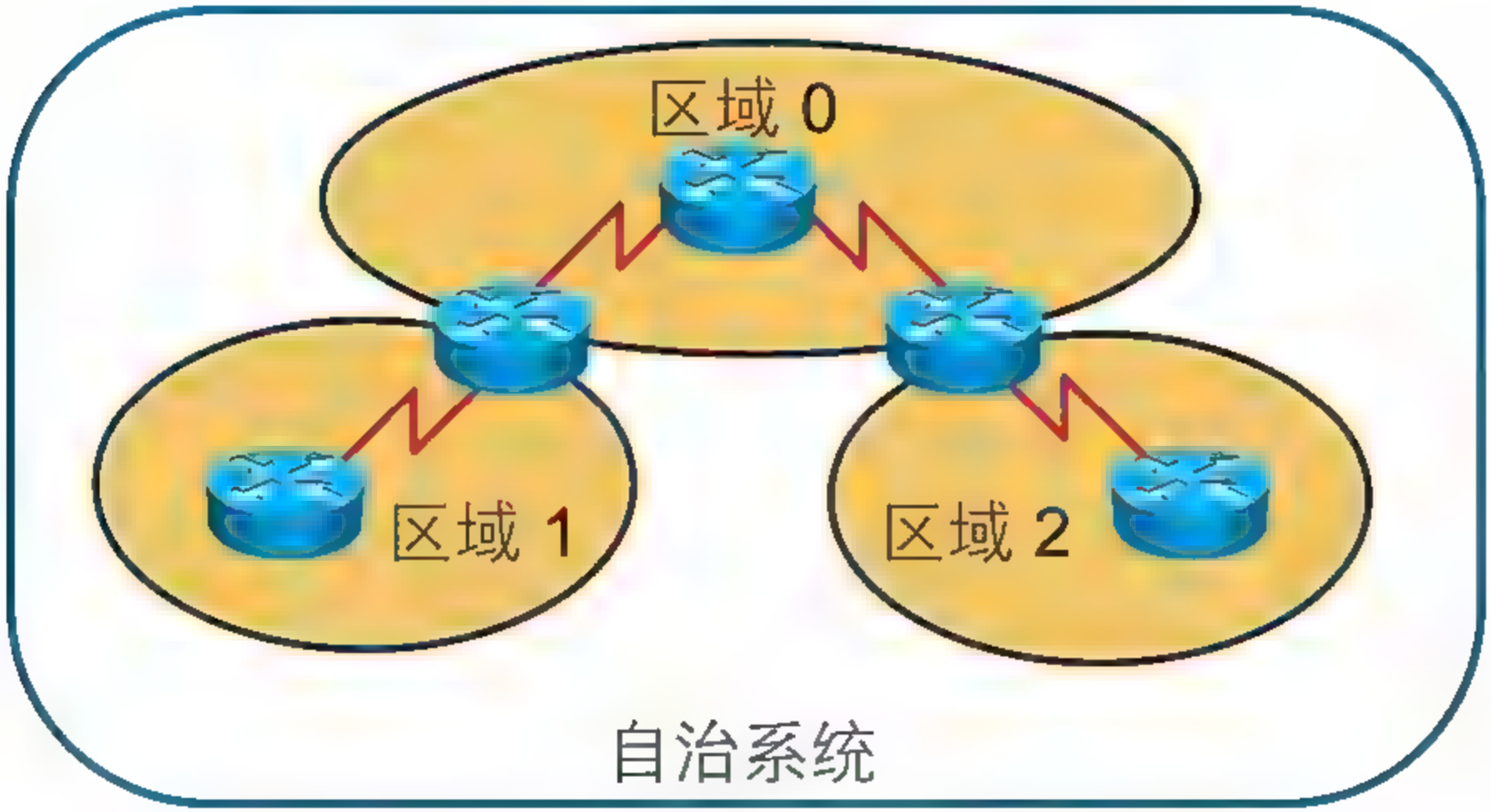
链路状态路由协议



LSA 初次泛洪后，链路状态路由器将向所有其它路由器传递由事件触发的较小链路状态更新。

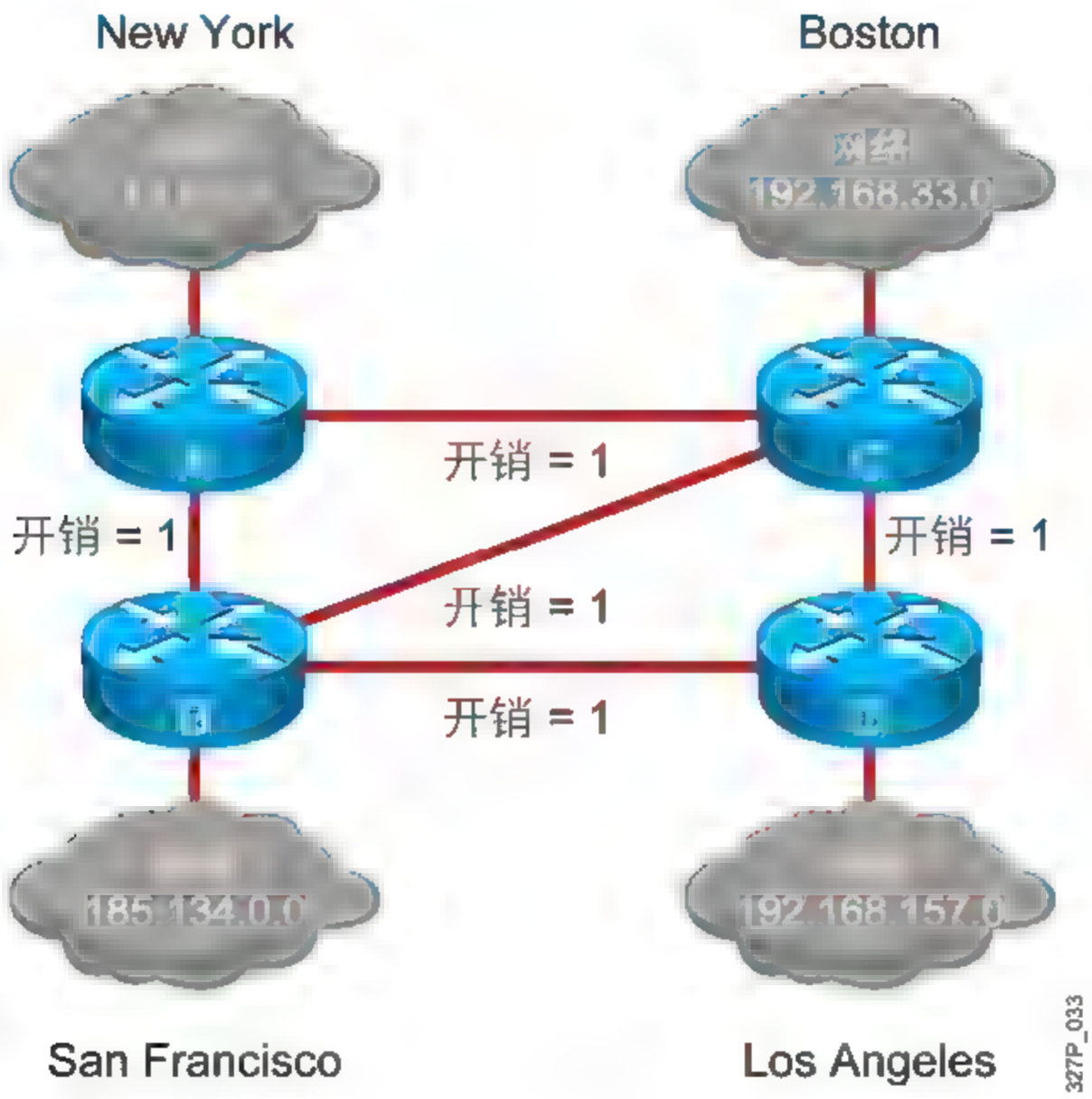
© 2008 Cisco Systems, Inc. 保留所有权利

OSPF 分层路由



- 包括区域和自治系统
- 最小化路由更新流量

链路状态路由协议算法



© 2008 Cisco Systems, Inc. 保留所有权利。

链路状态路由的优缺点

- 链路状态路由的优点：
  - 快速收敛：
    - 受影响的源会立即报告更改
  - 有效防止路由环路：
    - 路由器了解拓扑
    - 链路状态数据包是有序且经过确认的数据包
  - 分层网络设计优化了资源。

- 链路状态路由的缺点：
  - 需要大量资源：
    - 存储器（三个表：邻接、拓扑、转发）
    - CPU（Dijkstra 算法计算量很大，特别是存在许多不稳定因素时）
  - 要求非常严格的网络设计
  - 在对各种参数进行调整以及设计很复杂时，配置会非常复杂

总结

- 动态路由需要管理员配置距离矢量或链路状态路由协议。
- 距离矢量路由协议采用水平分割、路由毒化和抑制计时器等解决方案以防止路由环路。
- 链路状态路由协议比距离矢量路由协议更能适应大型网络基础架构，但需要更多的规划才能实施。

CISCO

实施 VLSM

中型路由网络构建

复习子网划分

为了标识子网，您需要从 IP 地址的主机 ID 部分“借用”一些位：

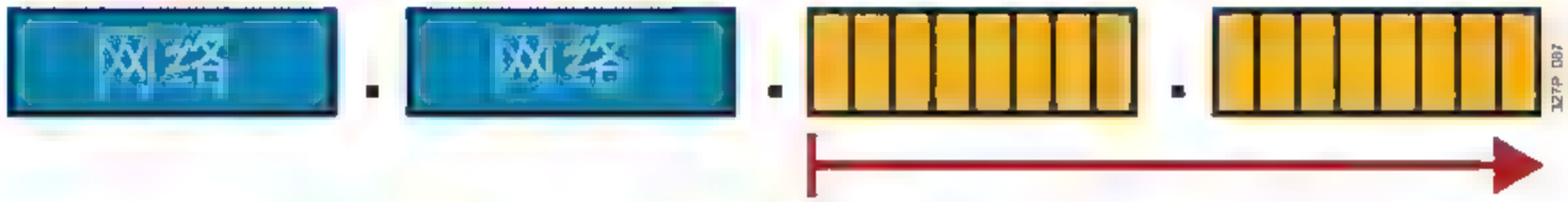
- 可用子网的数量取决于借用的位数。
  - 可用子网的数量 = 2^s，其中 *s* 是借用的位数。
- 每个子网中的可用主机的数量取决于*未*借用的主机 ID 的位数。
  - 每个子网中的可用主机的数量 = 2^h-2，其中 *h* 是未借用的主机位数。
  - 保留一个地址作为网络地址。
  - 保留一个地址作为广播地址。

C 类网络可能的子网数和主机数

1	2	7	126
2	4	6	62
3	8	5	30
4	16	4	14
5	32	3	6
6	64	2	2
7	128	1	0

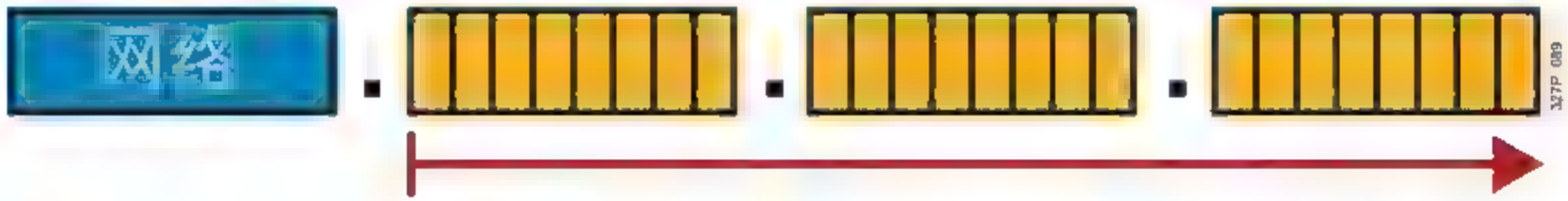
Systems Inc. 保留所有权利。

B 类网络可能的子网数和主机数



1	2	15	32,766
2	4	14	16,382
3	8	13	8,190
4	16	12	4,094
5	32	11	2,046
6	64	10	1,022
7	128	9	510
…	…	…	…

A 类网络可能的子网数和主机数



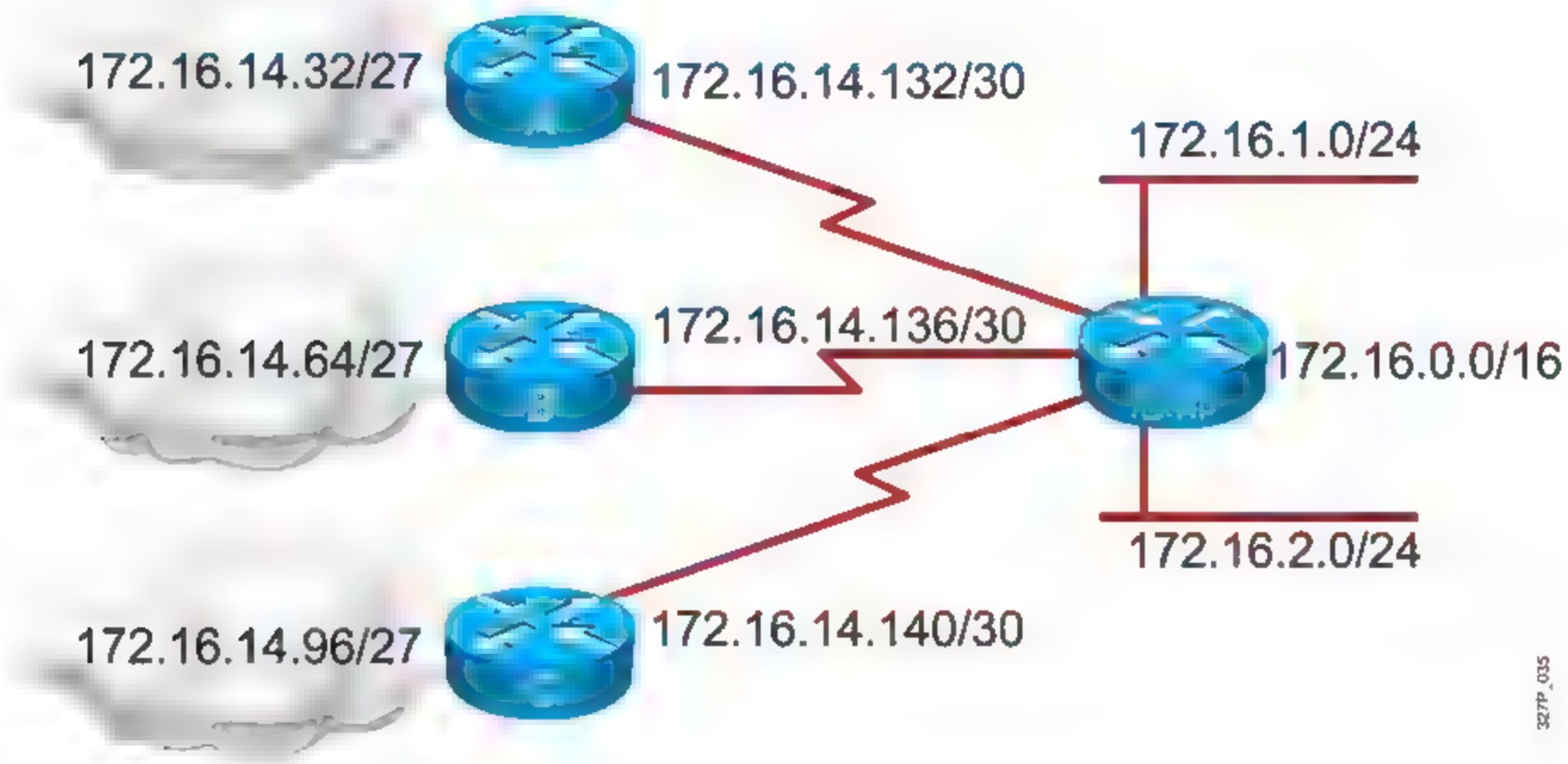
1	2	23	8,388,606
2	4	22	4,194,302
3	8	21	2,097,150
4	16	20	1,048,574
5	32	19	524,286
6	64	18	262,142
7	128	17	131,070
...	...	...	...

复习子网划分练习

使用私有网络地址 172.16.0.0./16 为网络创建子网，则网络可提供 100 个子网，并可最大化每个子网的主机地址数。

- 需要借用多少位？
- 新的子网掩码是多少？
- 前四个子网的地址是多少？
- 这四个子网的主机地址范围分别是多少？

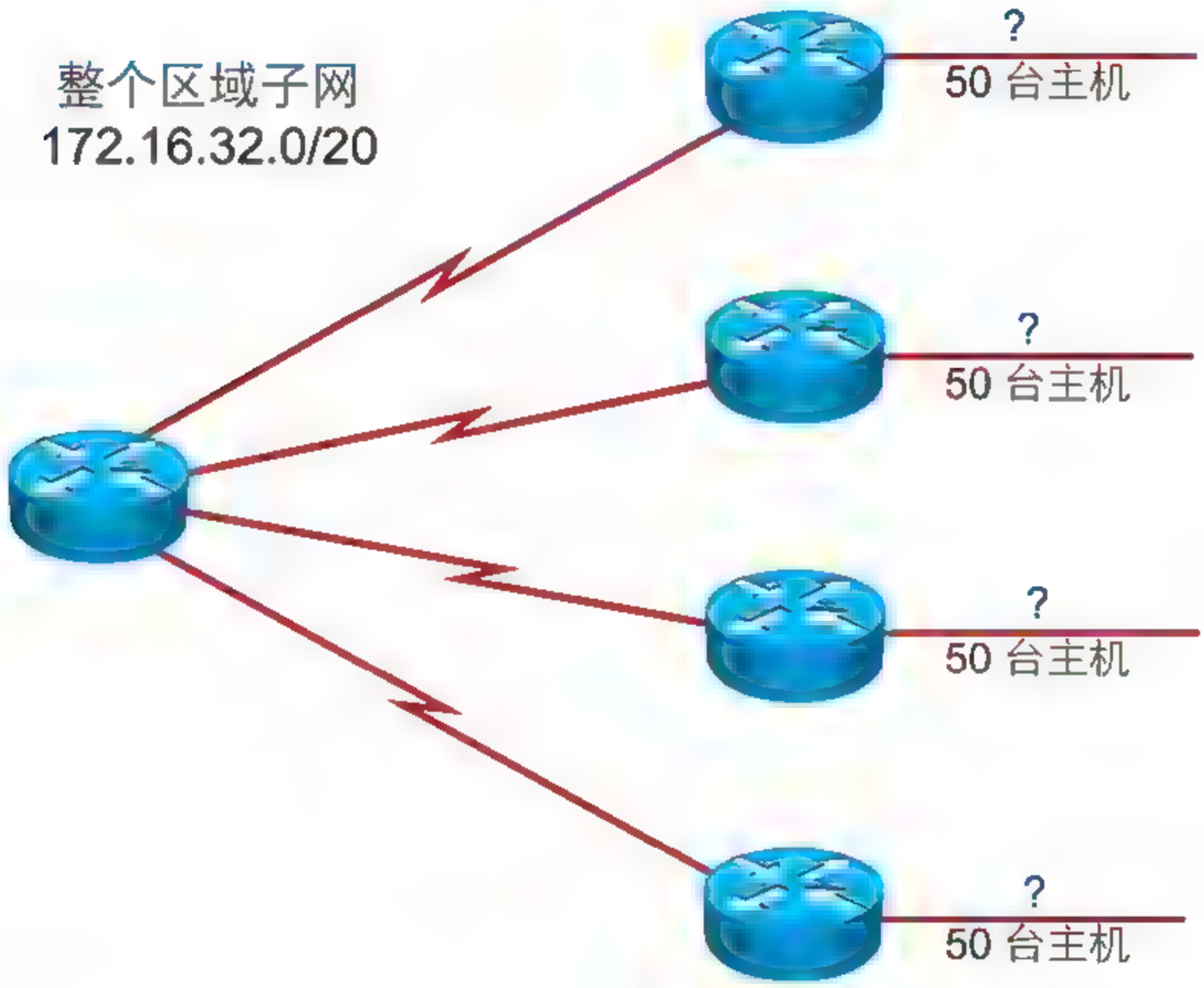
什么是可变长子网掩码？



子网 172.16.14.0/24 可以划分为更小的子网。

- 子网具有一个掩码 (/27)。
- 然后进一步将某个未使用的 /27 子网划分为多个 /30 子网。

运行中的 VLSM 示例



运行中的 VLSM 示例（续）

子网地址：172.16.32.0/20
二进制表示 10101100. 00010000.0010**0000.00000000**

VLSM 地址：172.16.32.0/26
二进制表示 10101100. 00010000.0010**0000.00**000000

第 1 个子网：	172.16	.0010	0000.00	000000=172.16.32.0/26
第 2 个子网：	172.16	.0010	0000.01	000000=172.16.32.64/26
第 3 个子网：	172.16	.0010	0000.10	000000=172.16.32.128/26
第 4 个子网：	172.16	.0010	0000.11	000000=172.16.32.192/26
第 5 个子网：	172.16	.0010	0001.00	000000=172.16.33.0/26
	网络	子网	VLSM 子网	主机

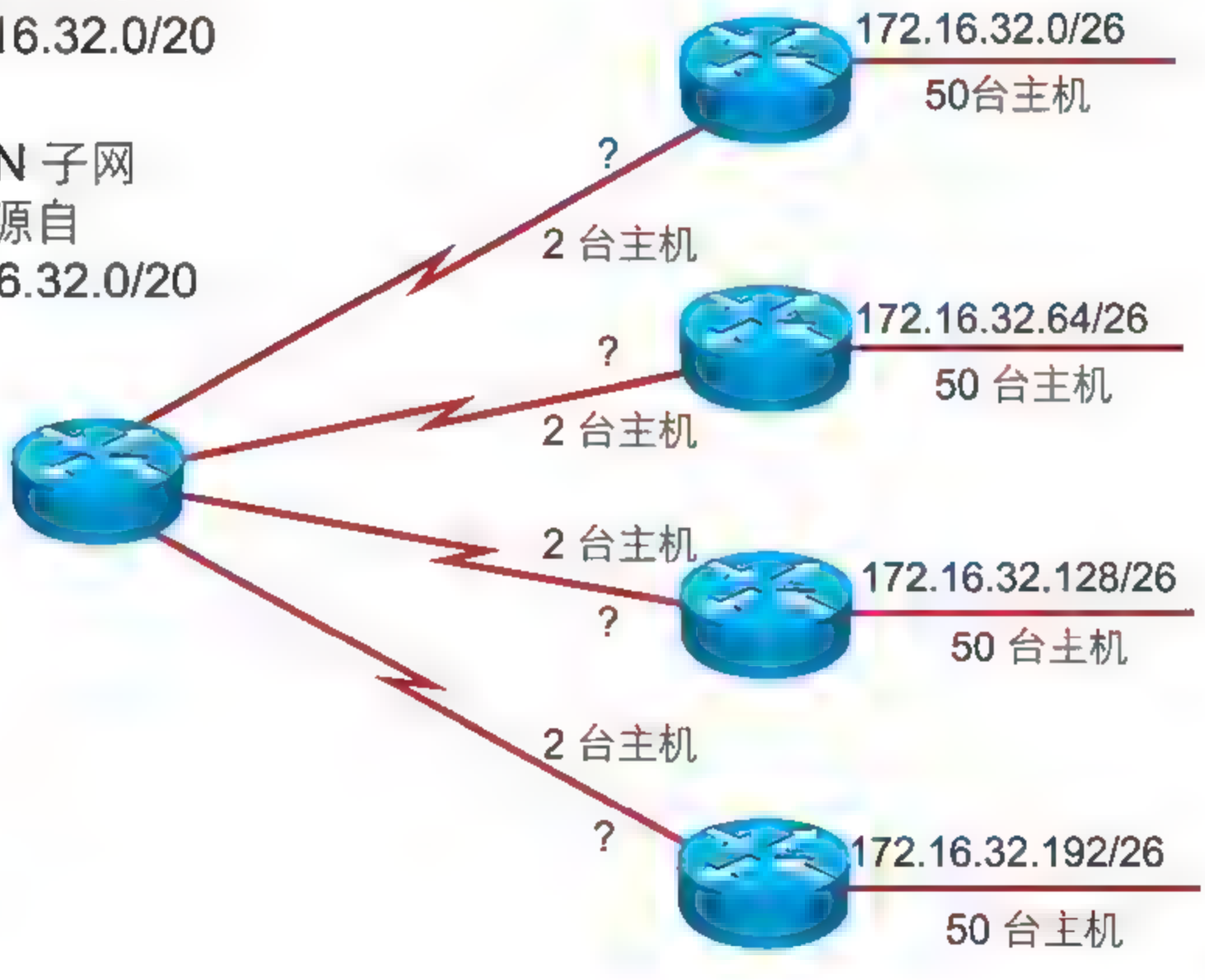
327P_091

© 2008 Cisco Systems, Inc. 保留所有权利。

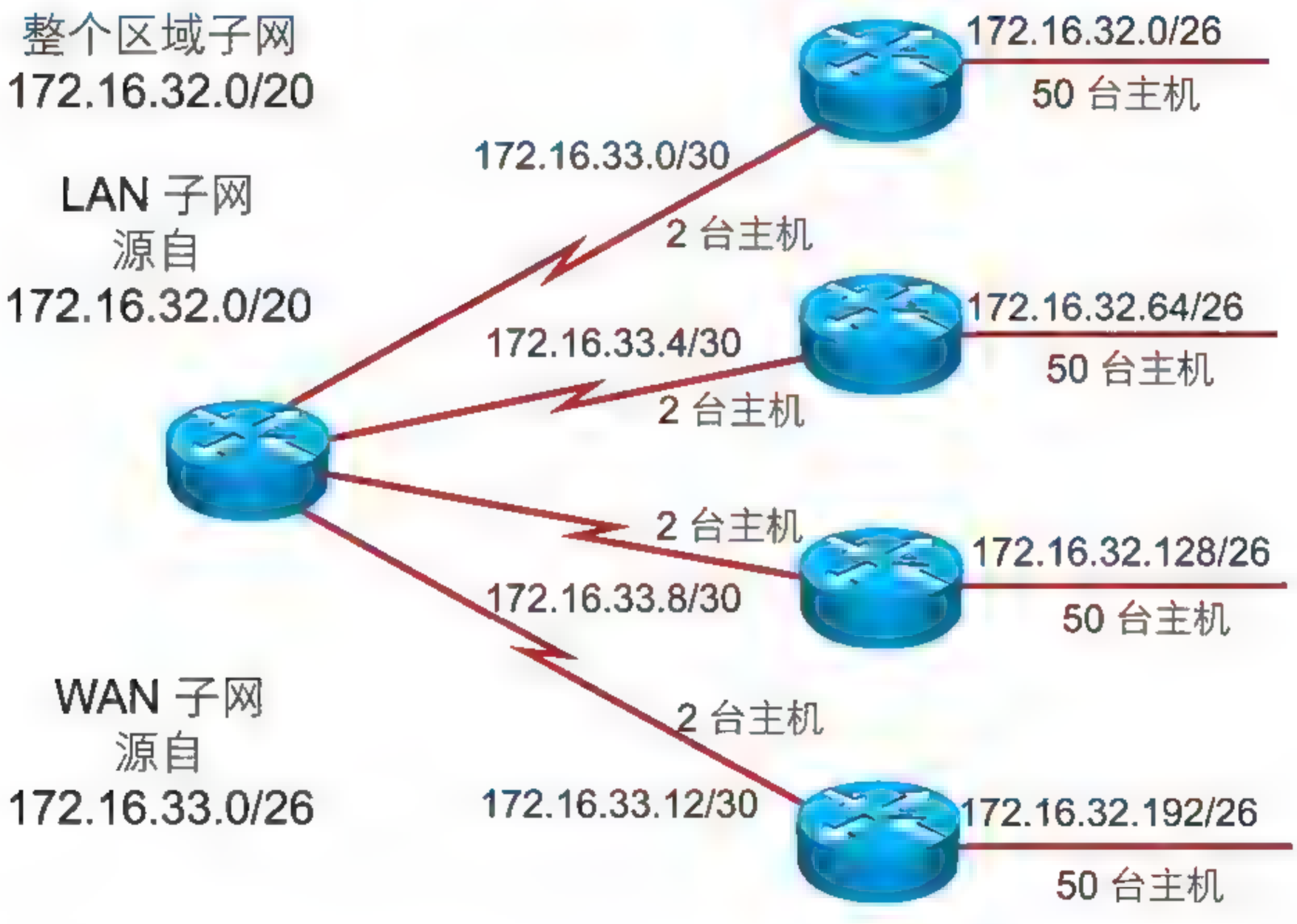
运行中的 VLSM 示例（续）

整个区域子网
172.16.32.0/20

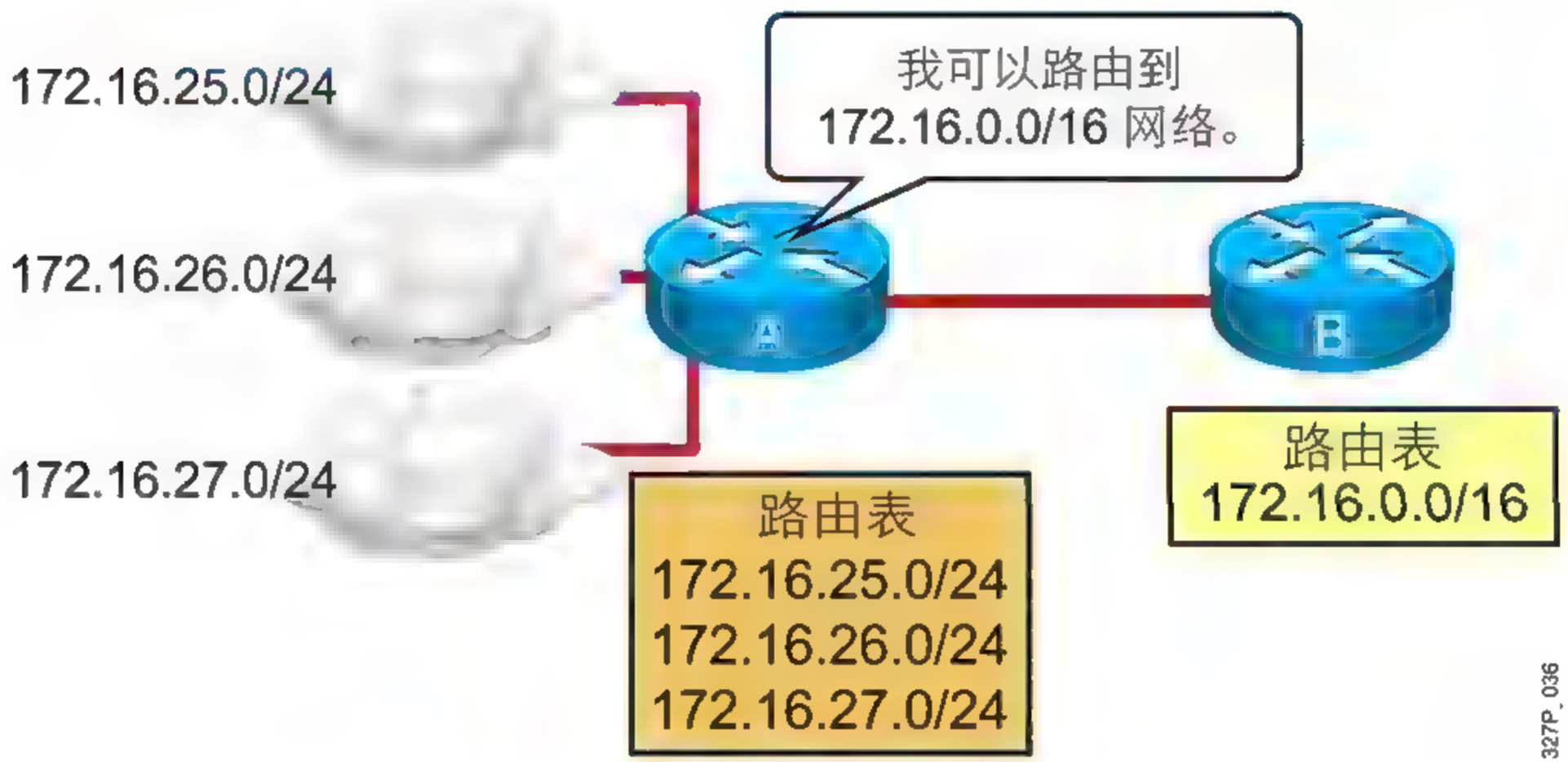
LAN 子网
源自
172.16.32.0/20



运行中的 VLSM 示例（续）



了解路由总结



路由协议可以将几个网络地址总结成一个地址。

有类路由概述

- 有类路由协议不会把子网掩码包括到路由通告中的网络。
- 在相同的网络中，假设子网掩码是一致的，整个网络具有一个子网掩码。
- 在外部网络之间交换总结路由。
- 有类路由协议的示例包括：
  - RIPv1
  - IGRP

注：有类路由协议是通常用于解决兼容性问题的原有路由协议。我们将以 RIP 第 1 版和内部网关路由协议 (IGRP) 为例进行介绍。

无类路由概述

- 在无类路由协议的通告中，同时包括网络地址和子网掩码。
- 无类路由协议支持 VLSM；一个网络可以具有多个掩码。
- 必须在网络中手动控制总结路由。
- 无类路由协议的示例包括：
  - RIPv2
  - EIGRP
  - OSPF
- 默认情况下 RIPv2 和 EIGRP 是有类路由协议，在外部网络之间交换总结路由。
  - no auto-summary 命令强制这些协议按照无类路由协议的方式工作。

在二进制八位数内总结

172.16.168.0/24 =	10101100	.	00010000	.	10101	000	.	00000000
172.16.169.0/24 =	172	.	16	.	10101	001	.	0
172.16.170.0/24 =	172	.	16	.	10101	010	.	0
172.16.171.0/24 =	172	.	16	.	10101	011	.	0
172.16.172.0/24 =	172	.	16	.	10101	100	.	0
172.16.173.0/24 =	172	.	16	.	10101	101	.	0
172.16.174.0/24 =	172	.	16	.	10101	110	.	0
172.16.175.0/24 =	172	.	16	.	10101	111	.	0

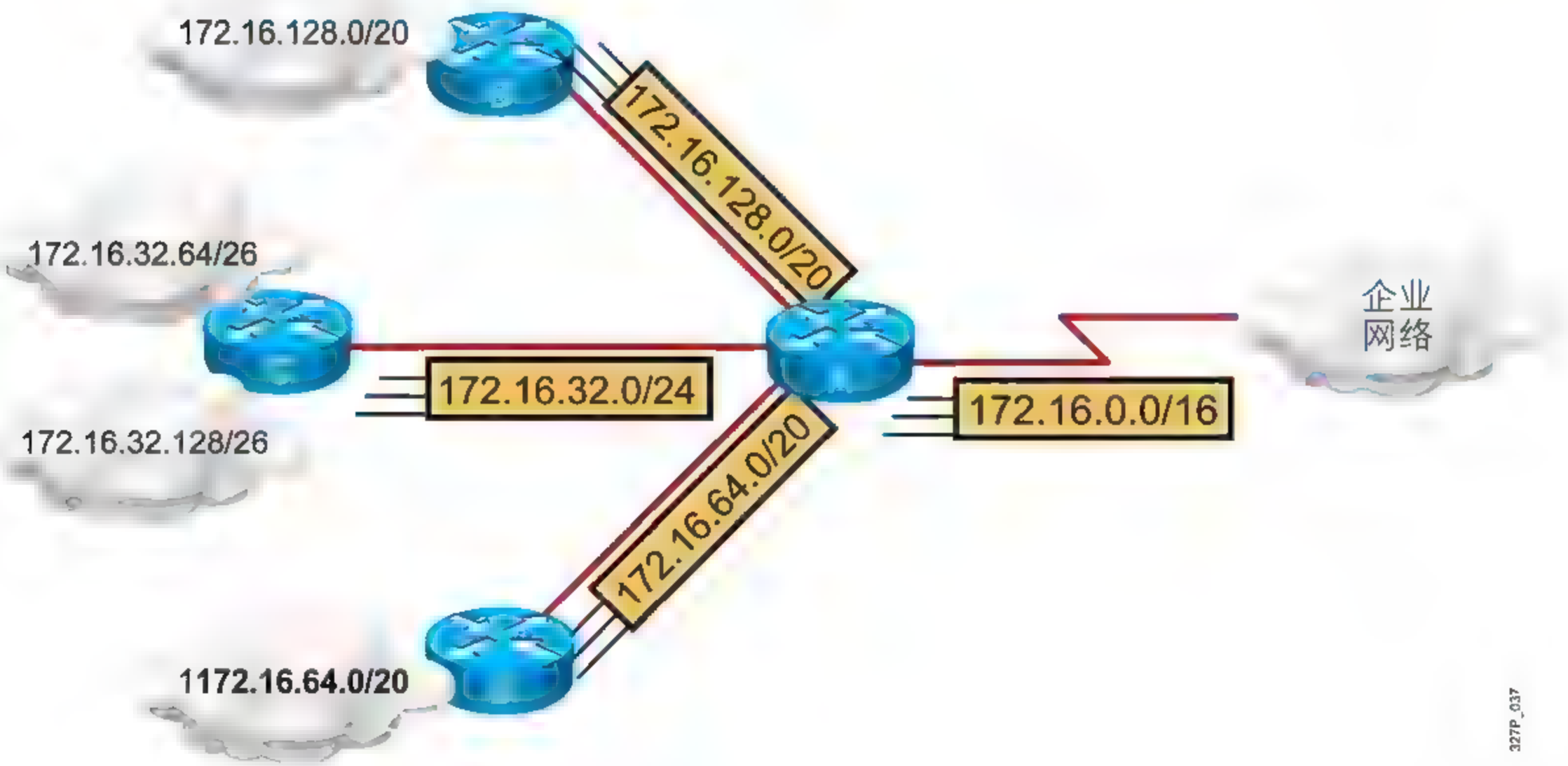
3279_092

相同位的数量 = 21
总结：172.16.168.0/21

不相同位的
数量 = 11

© 2008 Cisco Systems, Inc. 保留所有权利。

在用 VLSM 设计的网络中总结地址

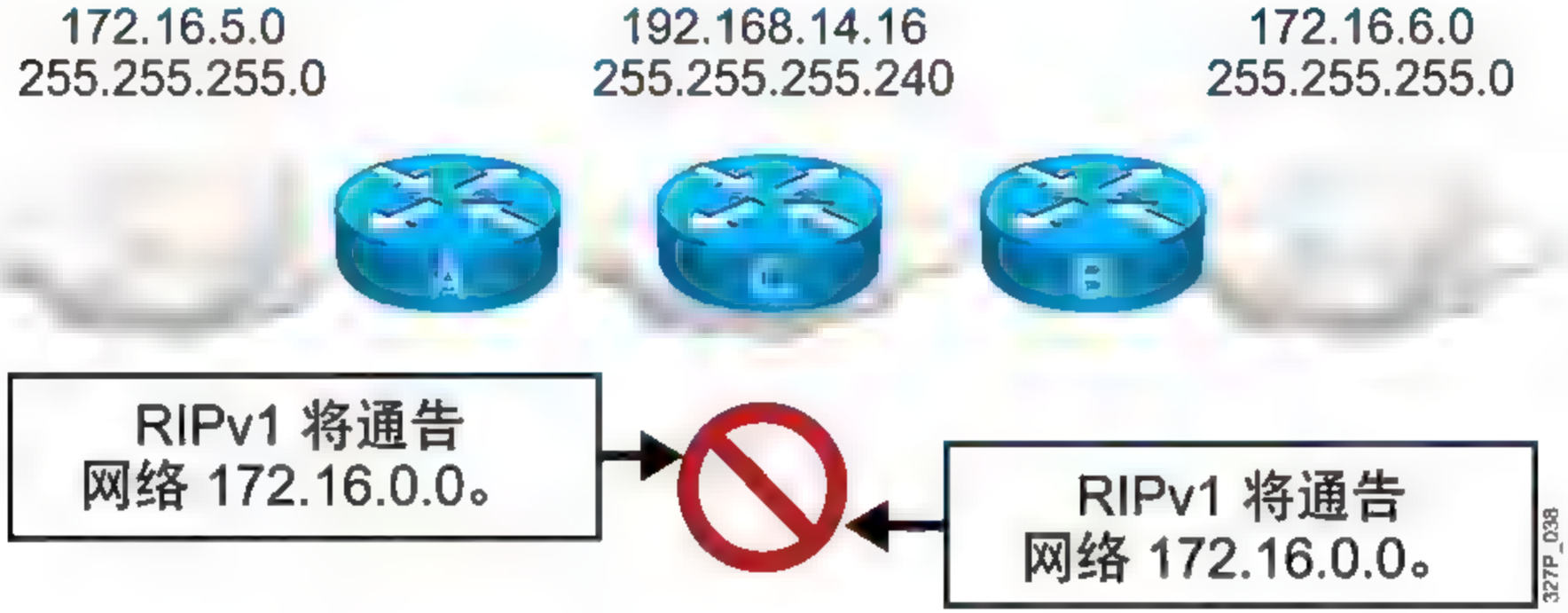


在 Cisco 路由器上执行路由总结操作

192.16.5.33	/32	主机
192.16.5.32	/27	子网
192.16.5.0	/24	网络
192.16.0.0	/16	网络块
0.0.0.0	/0	默认

- 支持特定于主机的路由、网络块和默认路由
- 路由器使用最长前缀匹配

在不连续网络中总结路由



- 有类 RIPv1 和 IGRP 不会通告子网，因此不支持不连续子网。
- 无类 OSPF、EIGRP 和 RIPv2 会通告子网，因此能够支持不连续子网。

总结

- 子网划分能将一个大型广播域划分为多个更易于管理的较小广播域，从而有效地分配地址。
- VLSM 可添加多层寻址层级以更有效地分配 IP 地址。
- 路由总结的优点包括拥有更小的路由表，并能隔离拓扑更改。

CISCO

单元总结

- 距离矢量路由算法会将它的整个路由表发送给邻居。链路状态路由算法会维护复杂的拓扑信息数据库，路由器可以使用此数据库来维护对远程路由器的完整感知。
- OSPF 是在许多网络中广泛部署的无类链路状态路由协议。EIGRP 是默认按照有类路由协议方式工作的无类路由协议。
- VLSM 允许在单个网络中存在多个级别的子网 IP 地址，并提供有效的 IP 地址分配。

CISCO

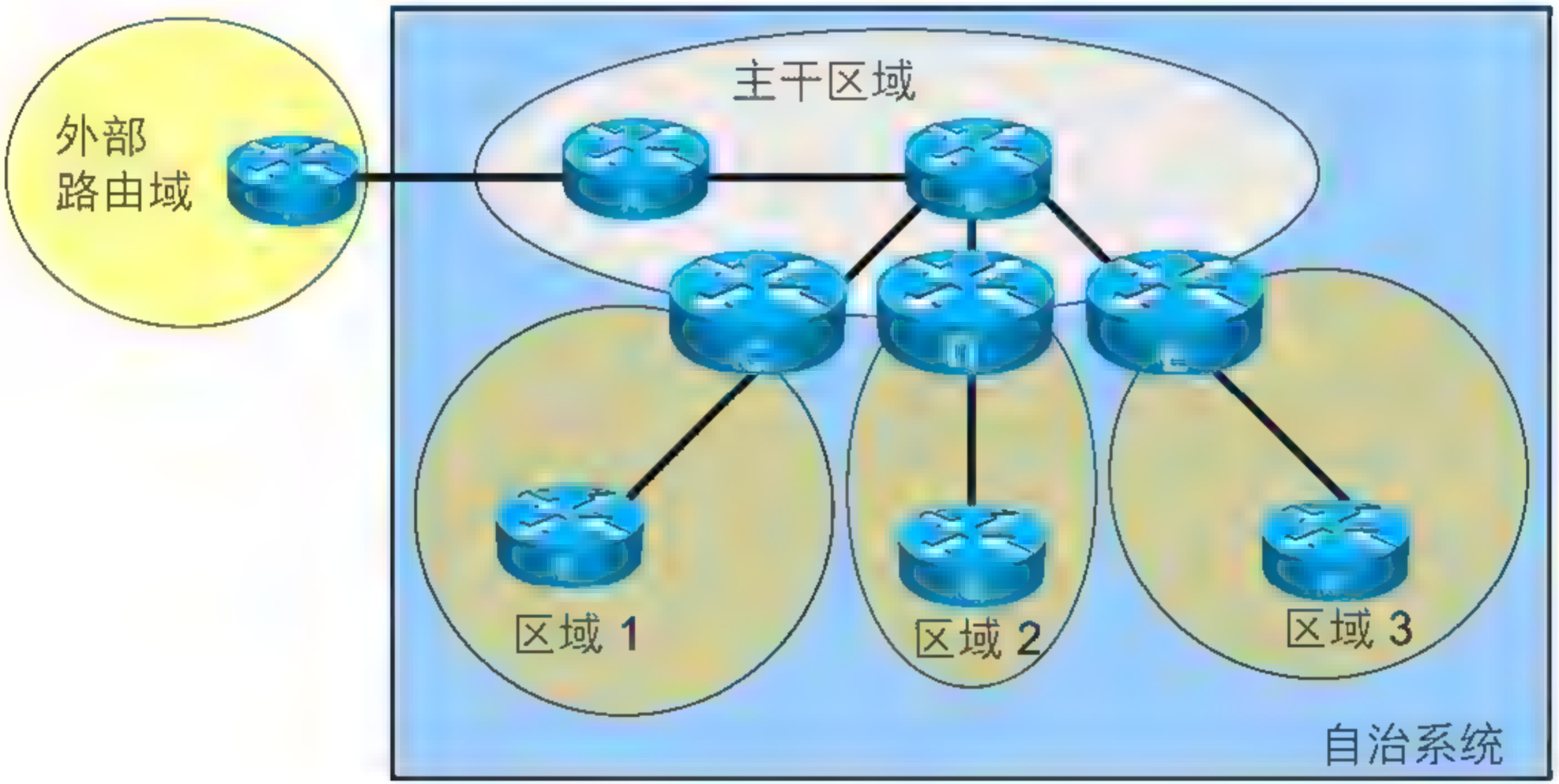
实施 OSPF

单区域 OSPF 实施

OSPF 概述

- 通过交换 hello 数据包来创建邻居关系
- 以传播 LSA 代替路由表更新
  - 链路：路由器接口
  - 状态：描述接口以及它与邻居路由器的关系
- 将 LSA 泛洪到区域中的所有 OSPF 路由器，而不仅是直连的路由器
- 收集由 OSPF 路由器生成的所有 LSA 以创建 OSPF 链路状态数据库
- 使用 SPF 算法计算到每个目的地的最短距离，并将其置于路由表中

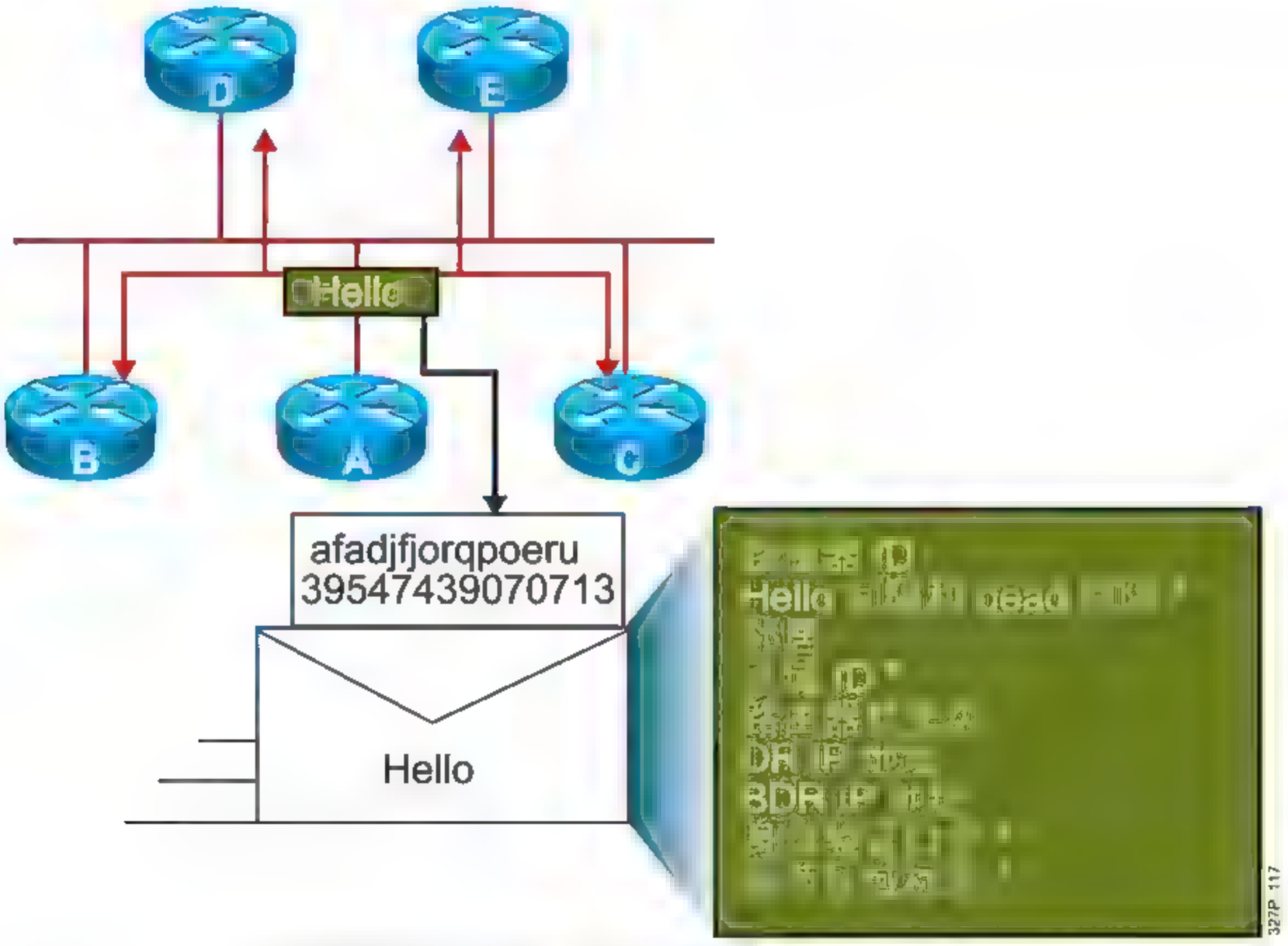
OSPF 层级示例



- 尽量减少路由表条目
- 使拓扑变化仅影响本区域内部

© 2006 Cisco Systems, Inc. 保留所有权利。

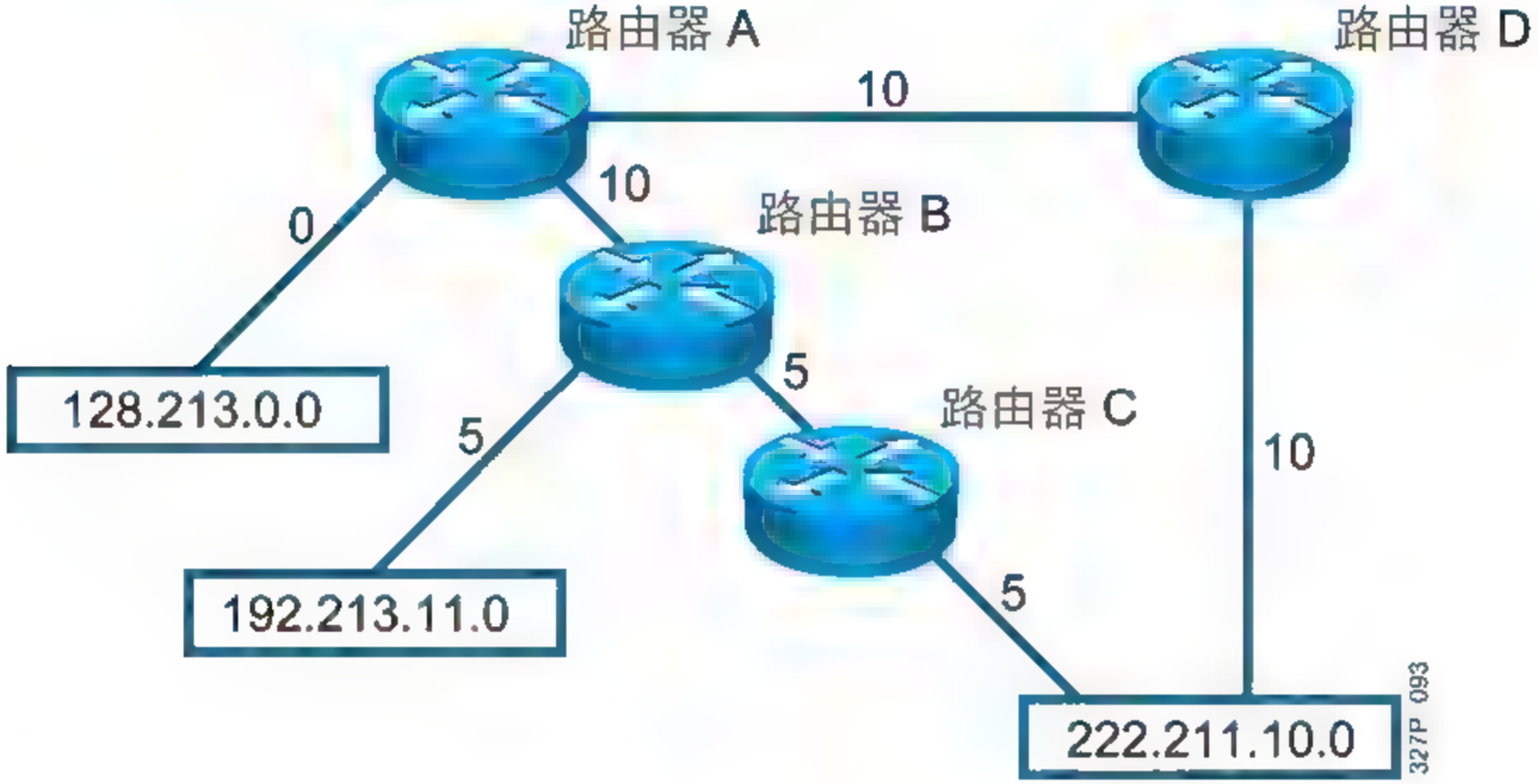
邻居关系：Hello 数据包



* 邻居路由器上的条目必须匹配

© 2008

SPF 算法



- 将每台路由器放置在树的根节点 ，并根据累计开销计算到达每个目的地的最短路径
- 开销 = 参考带宽 / 接口带宽 (b/s)

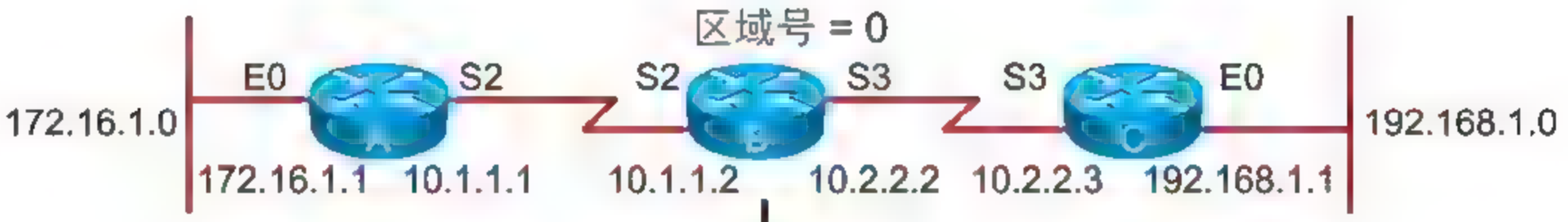
配置单区域 OSPF

```
RouterX(config)#
router ospf process-id
```

- 将 OSPF 定义为 IP 路由协议

```
RouterX(config-router)#
network address wildcard-mask area area-id
```

- 将网络分配到指定 OSPF 区域




```
router ospf 100
network 10.1.1.2 0.0.0.0 area 0
network 10.2.2.2 0.0.0.0 area 0
```

配置环回接口

未被通告的环回地址
例如：192.168.255.254
- 用作 OSPF 路由器 ID
- 节省地址空间
- 无法远程使用管理员路由器

已被通告的环回地址
例如：172.16.17.5
- 用作 OSPF 路由器 ID
- 使用地址空间
- 可以远程使用管理员路由器

327P 040

路由器 ID：

- 按照 OSPF 了解的路由器进行编号
- 默认值：OSPF 过程启动时活动接口上的最高 IP 地址
- 可以使用环回接口覆盖：任何活动环回接口上的最高 IP 地址
- 可以使用 **router-id** 命令手动设置

检验 OSPF 的配置

```
RouterX# show ip protocols
```

- 检验是否已配置 OSPF

```
RouterX# show ip route
```

- 显示路由器获知的所有路由

```
RouterX# show ip route

Codes:I - IGRP derived, R - RIP derived, O - OSPF derived,
C - connected, S - static, E - EGP derived, B - BGP derived,
E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
N2 - OSPF NSSA external type 2 route

Gateway of last resort is 10.119.254.240 to network 10.140.0.0

O 10.110.0.0 [110/5] via 10.119.254.6, 0:01:00, Ethernet2
O IA 10.67.10.0 [110/10] via 10.119.254.244, 0:02:22, Ethernet2
O 10.68.132.0 [110/5] via 10.119.254.6, 0:00:59, Ethernet2
O 10.130.0.0 [110/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.128.0.0 [170/10] via 10.119.254.244, 0:02:22, Ethernet2
```

检验 OSPF 的配置（续）

```
RouterX# show ip ospf
```

- 显示 OSPF 路由器 ID、计时器和统计信息

```
RouterX# show ip ospf
 Routing Process "ospf 50" with ID 10.64.0.2
<省略部分输出>

Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
  Area BACKBONE(0)
  Area BACKBONE(0)
  Area has no authentication
    SPF algorithm last executed 00:01:25.028 ago
    SPF algorithm executed 7 times
<省略部分输出>
```

检验 OSPF 的配置（续）

```
RouterX# show ip ospf interface
```

- 显示区域 ID 和邻接信息

```
RouterX# show ip ospf interface ethernet 0/0

Ethernet0/0 is up, line protocol is up
 Internet Address 192.168.1.2/24, Area 24
 Process ID 201, Router ID 192.168.1.2, Network Type BROADCAST, Cost: 10
 Transmit Delay is 1 sec, State DR, Priority 255
 Designated Router (ID) 192.168.1.2, Interface address 192.168.1.2
 Backup Designated router (ID) 4.4.4.4, Interface address 192.168.1.4
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:08
 Supports Link-local Signaling (LLS)
 Cisco NSF helper support enabled
 IETF NSF helper support enabled
 Index 1/3, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 2, maximum is 2
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 4.4.4.4  (Backup Designated Router
 Suppress hello for 0 neighbor(s)
```

检验 OSPF 的配置（续）

```
RouterX# show ip ospf neighbor
```

- 显示每个接口上的 OSPF 邻居信息

```
RouterX# show ip ospf neighbor

ID              Pri  State           Dead Time   Address         Interface
10.199.199.137  1    FULL/DR          0:00:31    192.168.80.37   FastEthernet0/0
172.16.48.1     1    FULL/DROTHER     0:00:33    172.16.48.1     FastEthernet0/1
172.16.48.200   1    FULL/DROTHER     0:00:33    172.16.48.200   FastEthernet0/1
10.199.199.137  5    FULL/DR          0:00:33    172.16.48.189   FastEthernet0/1
```

检验 OSPF 的配置（续）

```
RouterX# show ip ospf neighbor 10.199.199.137
Neighbor 10.199.199.137, interface address 192.168.80.37
In the area 0.0.0.0 via interface Ethernet0
Neighbor priority is 1, State is FULL
Options 2
Dead timer due in 0:00:32
Link State retransmission due in 0:00:04
Neighbor 10.199.199.137, interface address 172.16.48.189
In the area 0.0.0.0 via interface Fddi0
Neighbor priority is 5, State is FULL
Options 2
Dead timer due in 0:00:32
Link State retransmission due in 00:00:03
```

OSPF 调试命令

```
RouterX# debug ip ospf events

OSPF:hello with invalid timers on interface Ethernet0
hello interval received 10 configured 10
net mask received 255.255.255.0 configured 255.255.255.0
dead interval received 40 configured 30

OSPF:rcv. v:2 t:1 l:48 rid:200.0.0.117
   aid:0.0.0.0 chk:6AB2 aut:0 auk:

RouterX# debug ip ospf packet

OSPF:rcv. v:2 t:1 l:48 rid:200.0.0.116
aid:0.0.0.0 chk:0 aut:2 keyid:1 seq:0x0
```

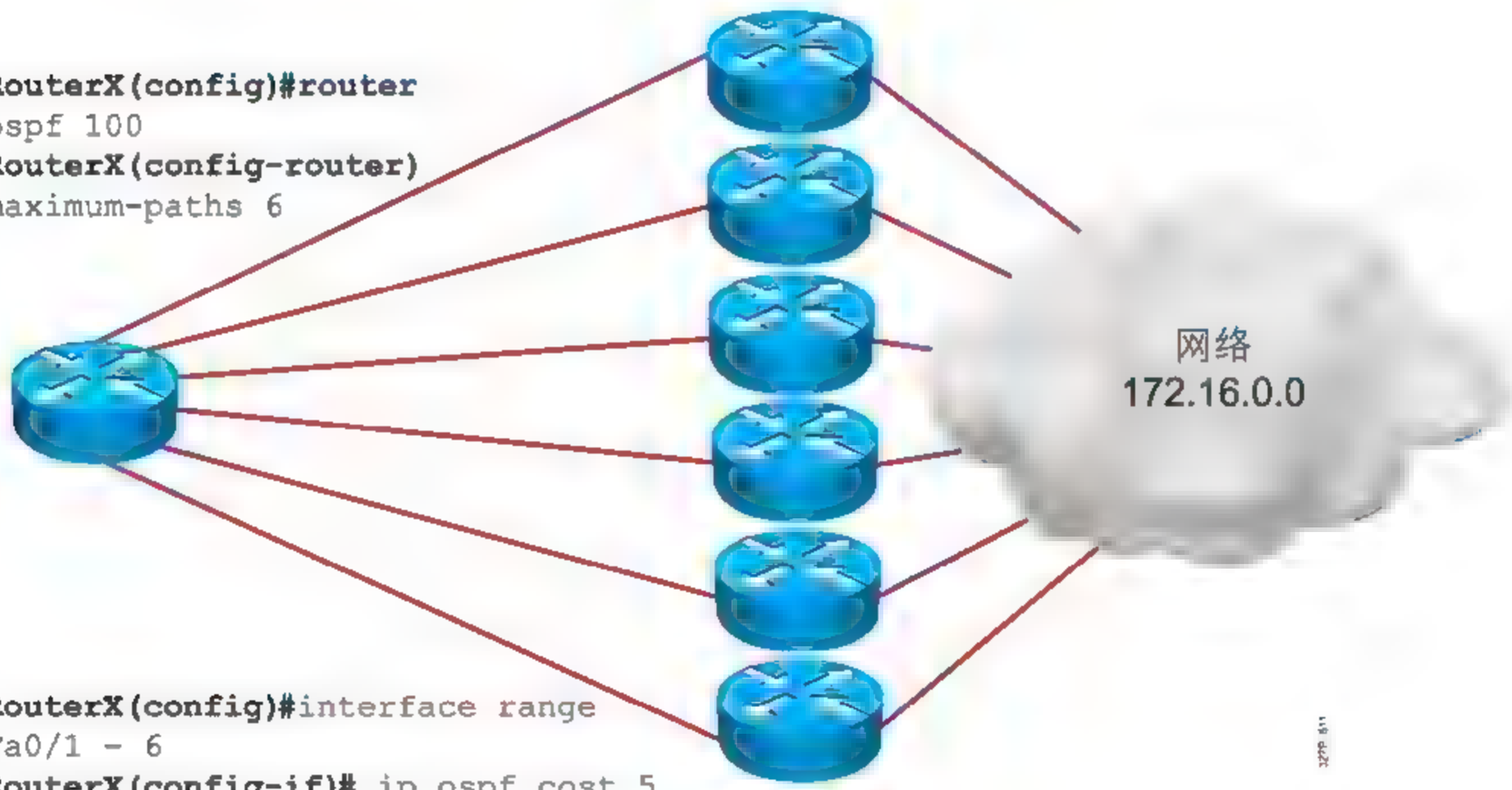
使用 OSPF 配置负载均衡

OSPF 负载均衡：

- 路径必须为等价路径
- 默认情况下，最多可在路由表中加入四条等价路径
- 通过更改配置，最多可以配置 16 条路径：
  - **(config-router)# maximum-paths <value>**
- 可更改特殊链路的开销以确保路径等价于负载均衡：
  - **(config-if)# ip ospf cost *<value>***

使用 OSPF 配置负载均衡（续）

```
RouterX(config)#router
ospf 100
RouterX(config-router)
maximum-paths 6
```




```
RouterX(config)#interface range
Fa0/1 - 6
RouterX(config-if)# ip ospf cost 5
```

© 2008 Cisco Systems, Inc. 保留所有权利。

OSPF 身份验证

- OSPF 支持以下几种类型的身份验证：
  - 空（无身份验证）
  - 明文（或简单）口令身份验证
  - MD5 身份验证
- 路由器生成并检查每个 OSPF 数据包。
- 路由器验证接收到的每个路由更新数据包的来源。
- 配置“密钥”（口令）；每个参与的邻居都必须配置相同的密钥。

配置 OSPF 明文口令身份验证

```
RouterX(config-if)#
ip ospf authentication-key password
```

- 分配用于邻居路由器的口令

```
RouterX(config-if)#
ip ospf authentication [message-digest | null]
```

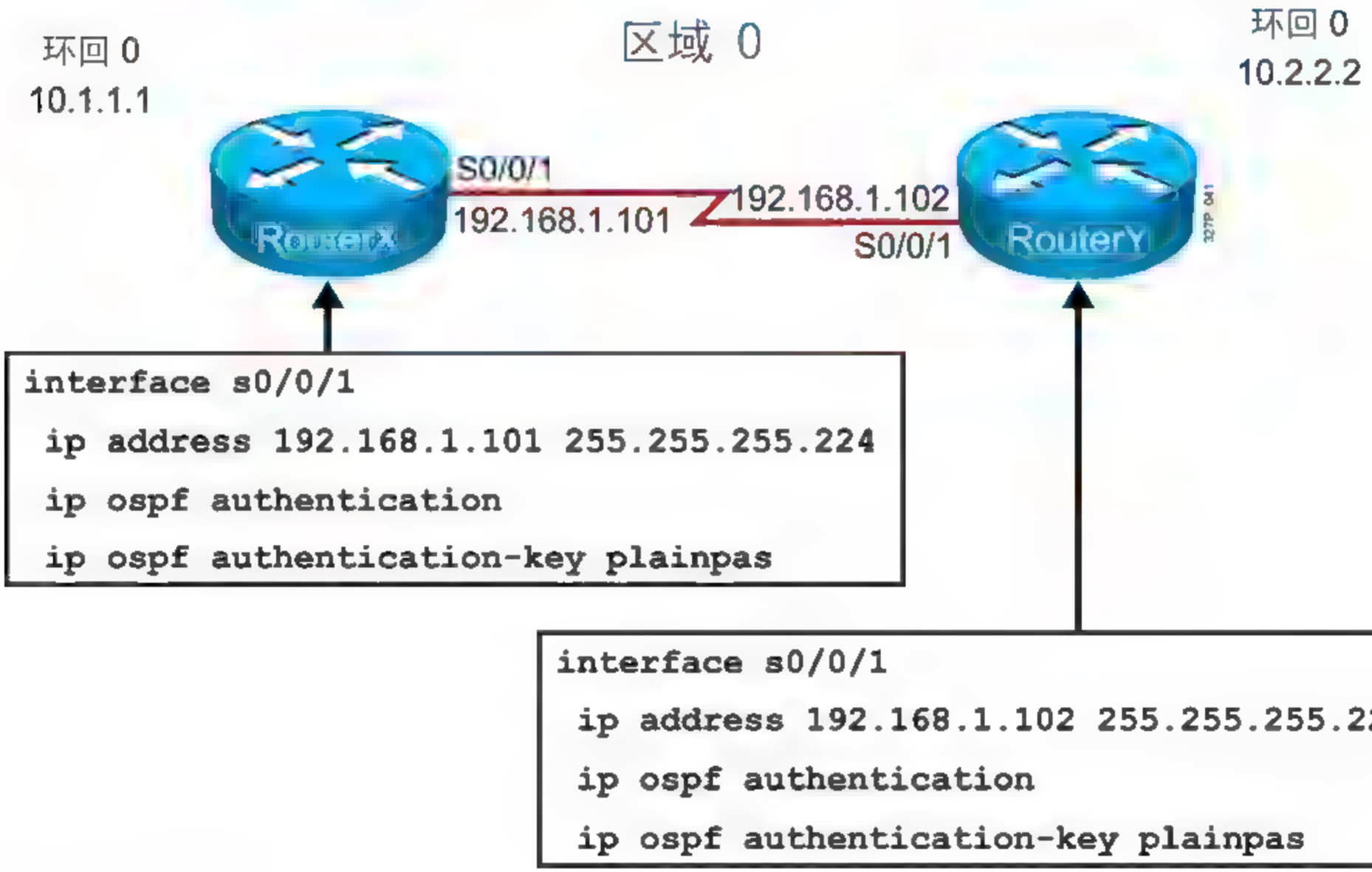
- 指定接口的身份验证类型（如 Cisco IOS 版本 12.0）

或者

```
RouterX(config-router)#
area area-id authentication [message-digest]
```

- 指定区域的身份验证类型

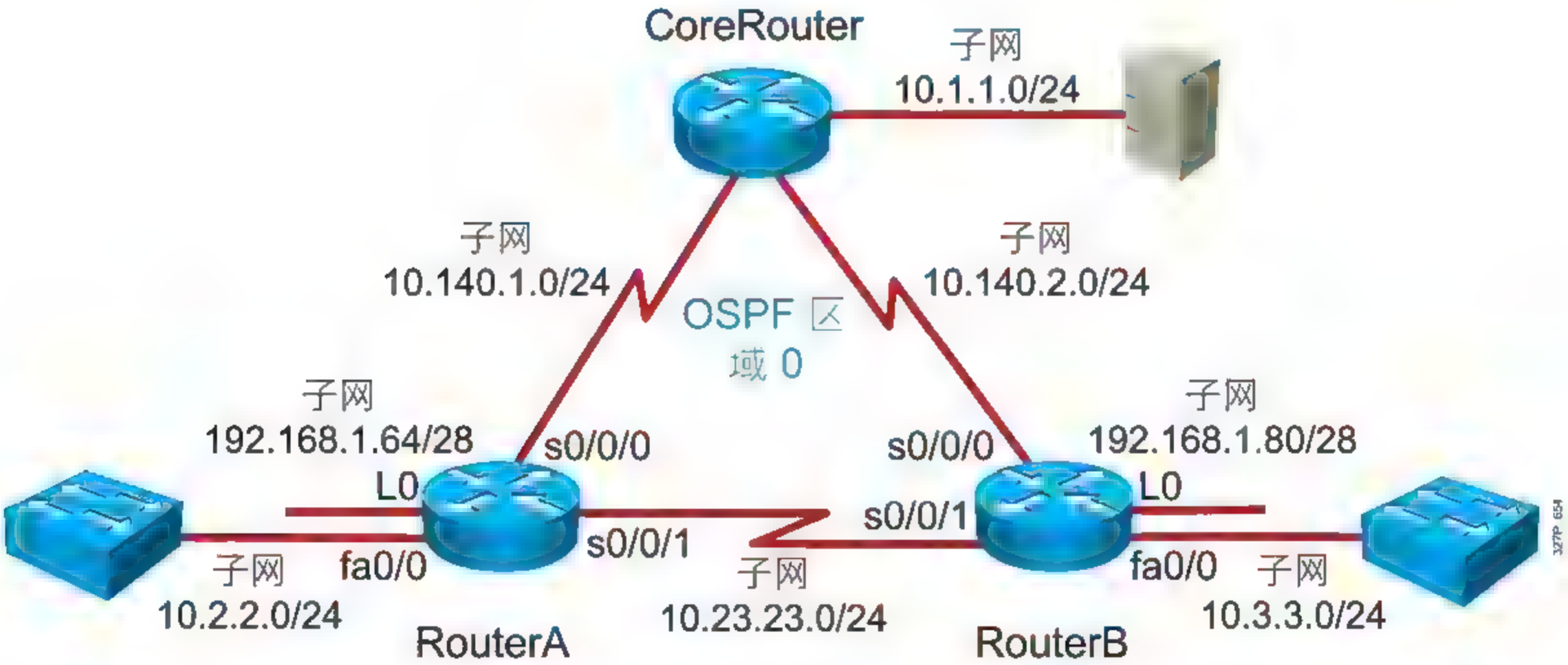
明文口令身份验证配置示例



检验明文口令身份验证

```
RouterX#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.2.2          0   FULL/  -        00:00:32    192.168.1.102   Serial0/0/1

RouterX# show ip route
<省略部分输出>
Gateway of last resort is not set
  10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O       10.2.2.2/32 [110/782] via 192.168.1.102, 00:01:17, Serial0/0/1
C       10.1.1.0/24 is directly connected, Loopback0
  192.168.1.0/27 is subnetted, 1 subnets
C       192.168.1.96 is directly connected, Serial0/0/1

RouterX#ping 10.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

可视目标 4-1：实施 OSPF



总结

- OSPF 是无类链路状态路由协议，它使用区域层级以加速收敛。
- OSPF 相互交换 hello 数据包以在路由器之间建立相邻邻接。
- SPF 算法使用开销度量确定最佳路径。开销越低，路径越好。
- **router ospf process-id** 命令用于在路由器上启用 OSPF。
- 使用环回接口保持 OSPF 路由器 ID 的一致性。
- **show ip ospf neighbor** 命令显示每个接口的 OSPF 邻居信息。
- 命令 **debug ip ospf events** 和 **debug ip ospf packets** 可用于排除 OSPF 故障。
- 默认情况下，OSPF 将通过最多四条等开销度量路径进行负载均衡。
- 有两类 OSPF 身份验证：明文和 MD5。

CISCO

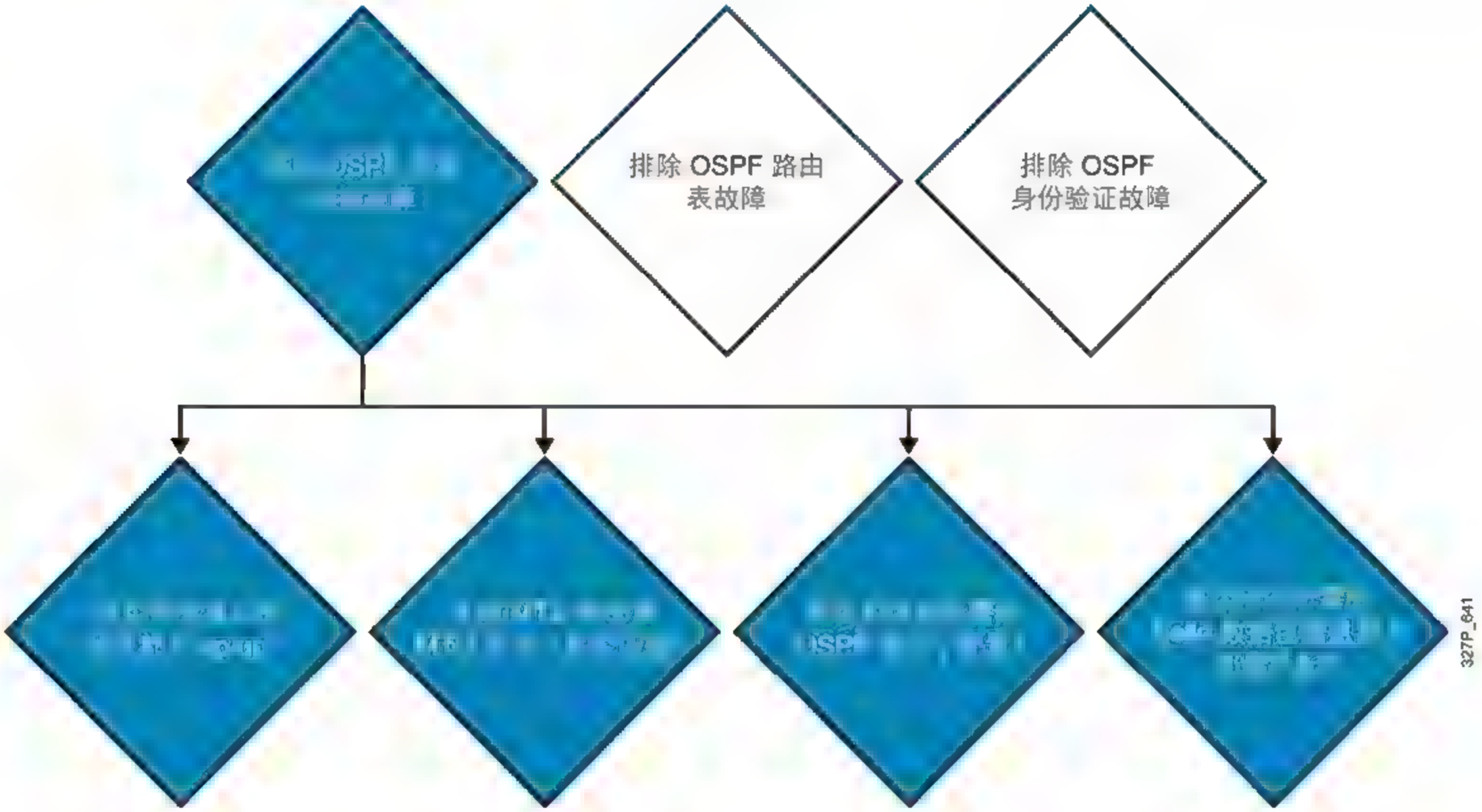
OSPF 故障排除

单区域 OSPF 实施

OSPF 故障排除组件

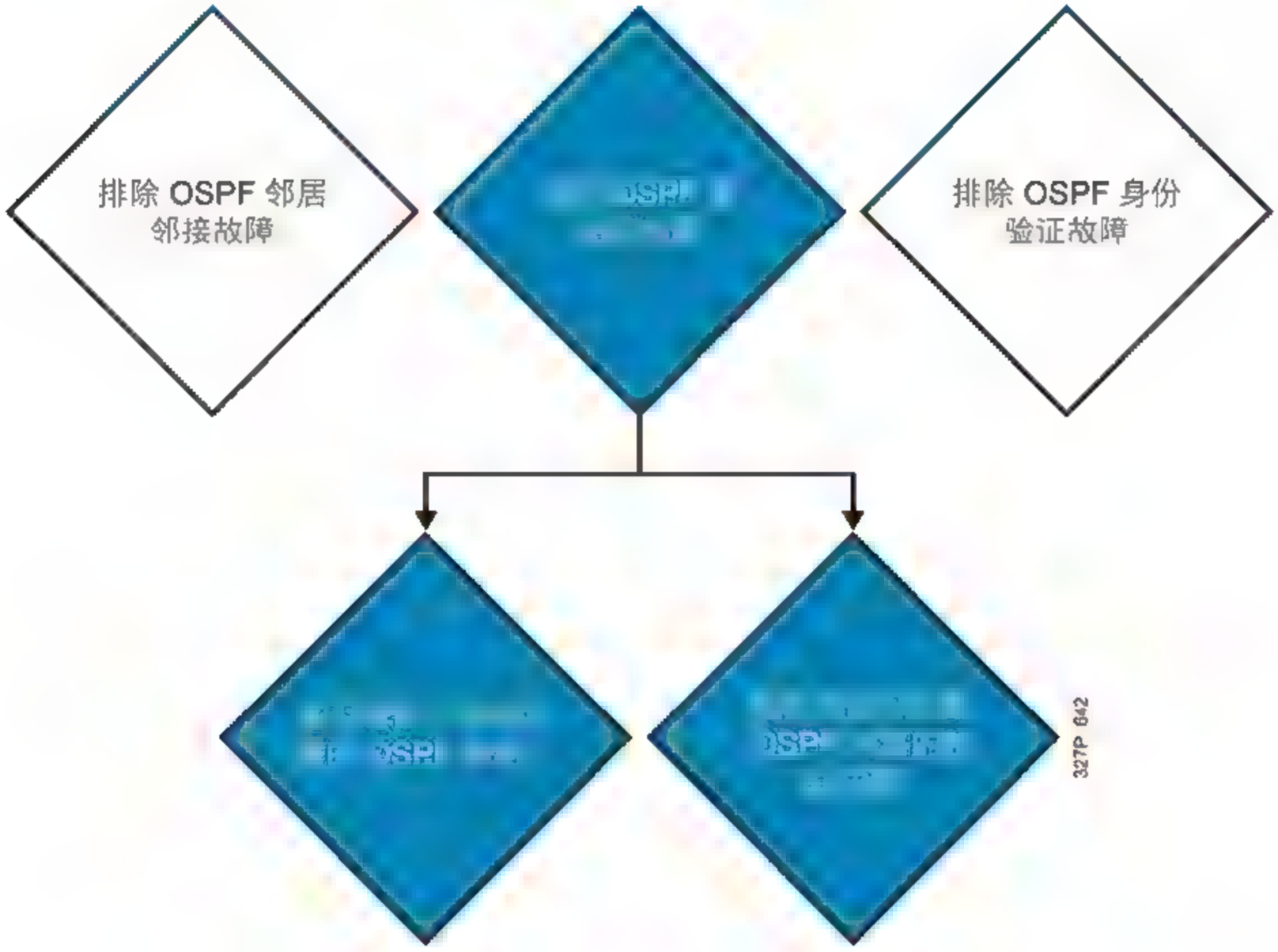
© 2008 Cisco Systems, Inc. 保留所有权利。

OSPF 邻居邻接故障排除



© 2008 Cisco Systems, Inc. 保留所有权利。

OSPF 路由表故障排除



© 2008 Cisco Systems, Inc. 保留所有权利。

排除明文口令身份验证故障

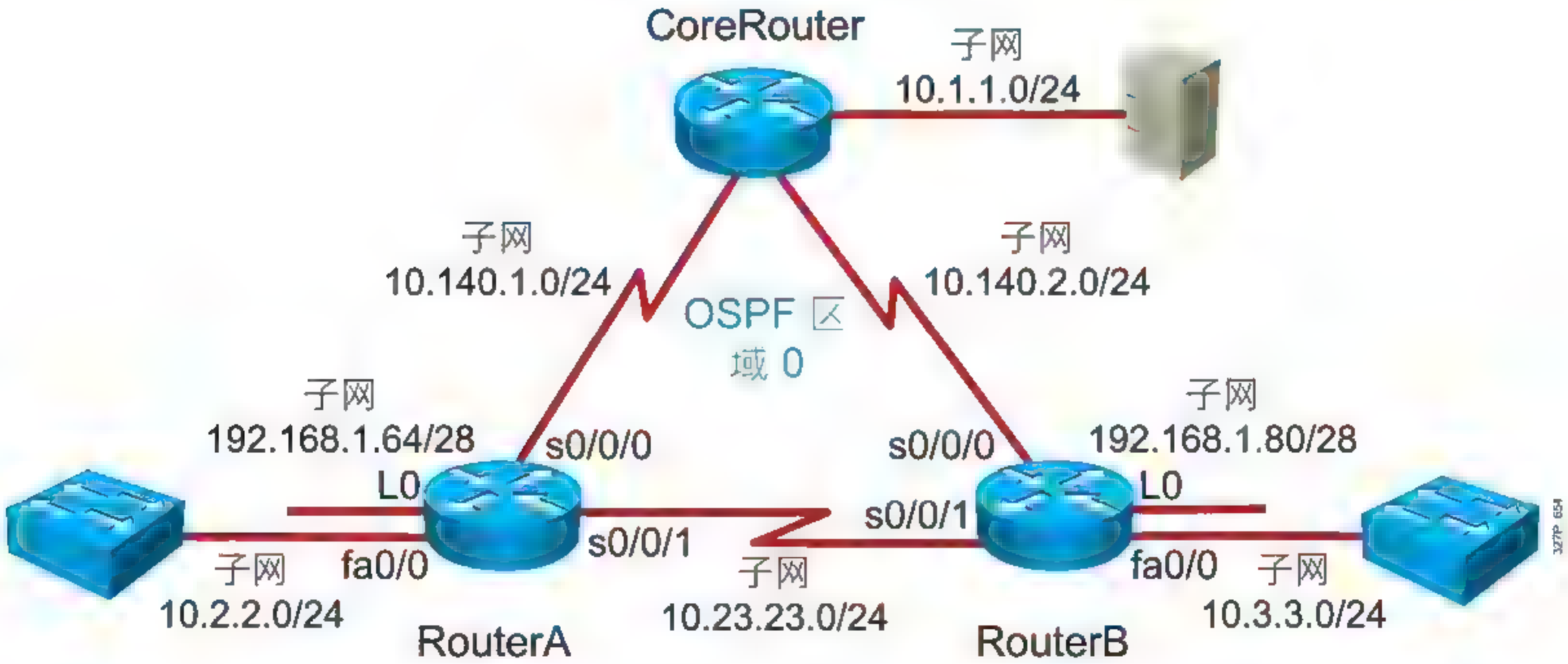
- routerX 采用明文口令身份验证，routerY 不采用身份验证

```
RouterX#debug ip ospf adj
*Feb 17 18:51:31.242:OSPF:Rcv pkt from 192.168.1.102, Serial0/0/1 :
Mismatch Authentication type.Input packet specified type 0, we use type 1

RouterY#debug ip ospf adj
*Feb 17 18:50:43.046:OSPF:Rcv pkt from 192.168.1.101, Serial0/0/1 :
Mismatch Authentication type.Input packet specified type 1, we use type 0
```

- routerX 和 routerY 都采用身份验证，但口令不同

```
RouterX#debug ip osp adj
*Feb 17 18:54:01.238:OSPF:Rcv pkt from 192.168.1.102, Serial0/0/1 :
Mismatch Authentication Key - Clear Text

RouterY#debug ip ospf adj
*Feb 17 18:53:13.050:OSPF:Rcv pkt from 192.168.1.101, Serial0/0/1 :
Mismatch Authentication Key - Clear Text
```

可视目标 4-2：
OSPF 故障排除



总结

- OSPF 故障排除涉及检查邻居邻接、路由表和身份验证的问题。
- 使用 **show ip interface** 命令检验 OSPF 接口的 MTU。
- 使用 **show ip ospf interface** 命令来帮助排除在接口上 OSPF 是否可用的故障。
- 使用 **debug ip ospf adj** 命令排除 OSPF 身份验证故障。

CISCO

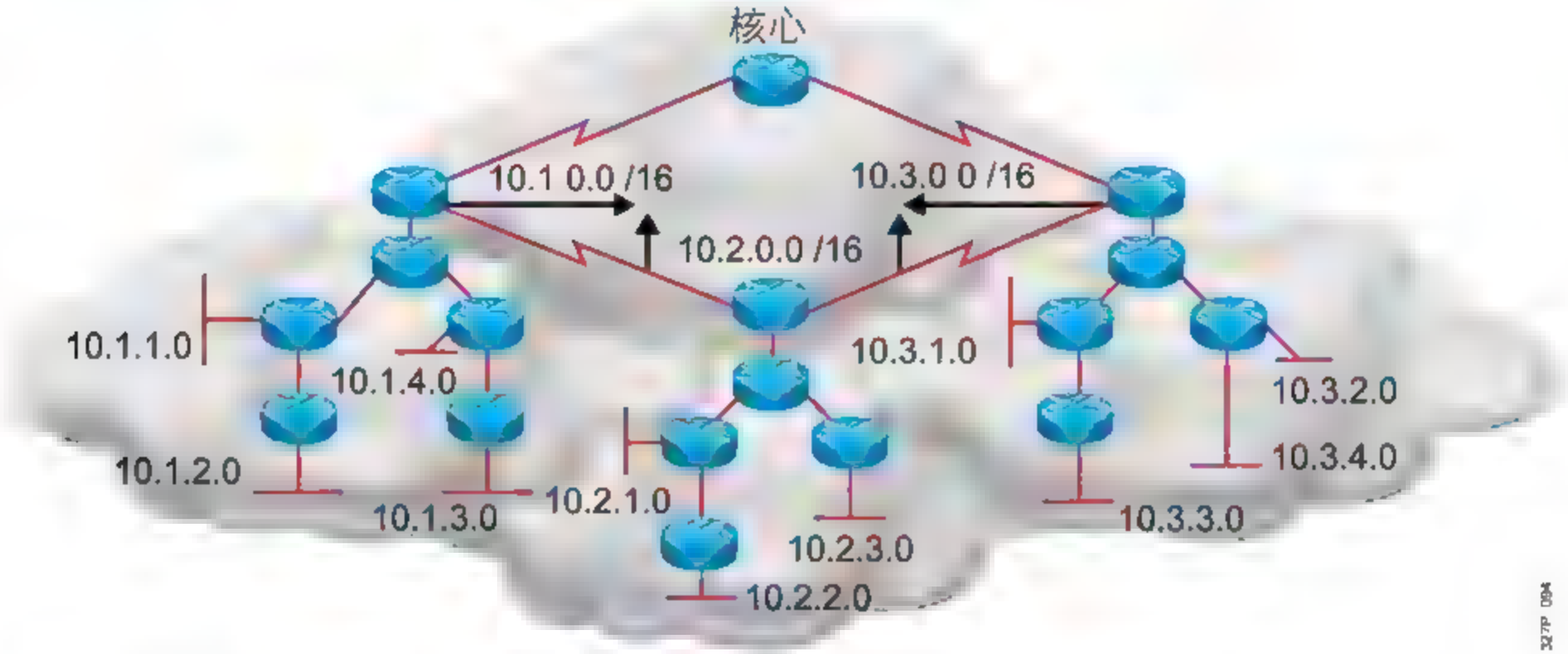
单元总结

- OSPF 的路由算法维护复杂的拓扑信息数据库，路由器使用该数据库维护对远程路由器的完整感知。
- OSPF 是在许多网络中广泛部署的无类链路状态路由协议。
- 在 Cisco 路由器中，OSPF 默认在四条相等度量路径上进行负载均衡。
- OSPF 支持明文身份验证和 MD5 身份验证。
- 存在多个用于排除 OSPF 故障的组件，包括 OSPF 邻居邻接和路由表。

实施 EIGRP

EIGRP 实施

EIGRP 的特点



- 高级距离矢量
- 快速收敛
- 100% 无回路的无类路由
- 配置简单
- 逐步更新
- 在开销相等和不相等的路径上实现负载平衡

- 网络设计灵活
- 用组播地址和单播地址代替广播地址
- 支持 VLSM 和不连续的子网
- 在 Internet 网络中的任意点手动总结
- 支持多种网络层协议

EIGRP 表

© 2008 Cisco Systems, Inc. 保留所有权利。

EIGRP 路径计算（路由器 C）

IP EIGRP 邻居表

下一跳路由器	接口
路由器 A	Ethernet 0
路由器 B	Ethernet 1

IP EIGRP 拓扑表

网络	可行距离（EIGRP 度量）	通告距离	EIGRP 邻居	
10.1.1.0 /24	2000	1000	路由器 A (E0)	← 后继
10.1.1.0 /24	2500	1500	路由器 B (E1)	← 可行后继

The IP 路由表

网络	度量（可行距离）	出站接口	下一跳（EIGRP 邻居）
10.1.1.0 /24	2000	Ethernet 0	路由器 A

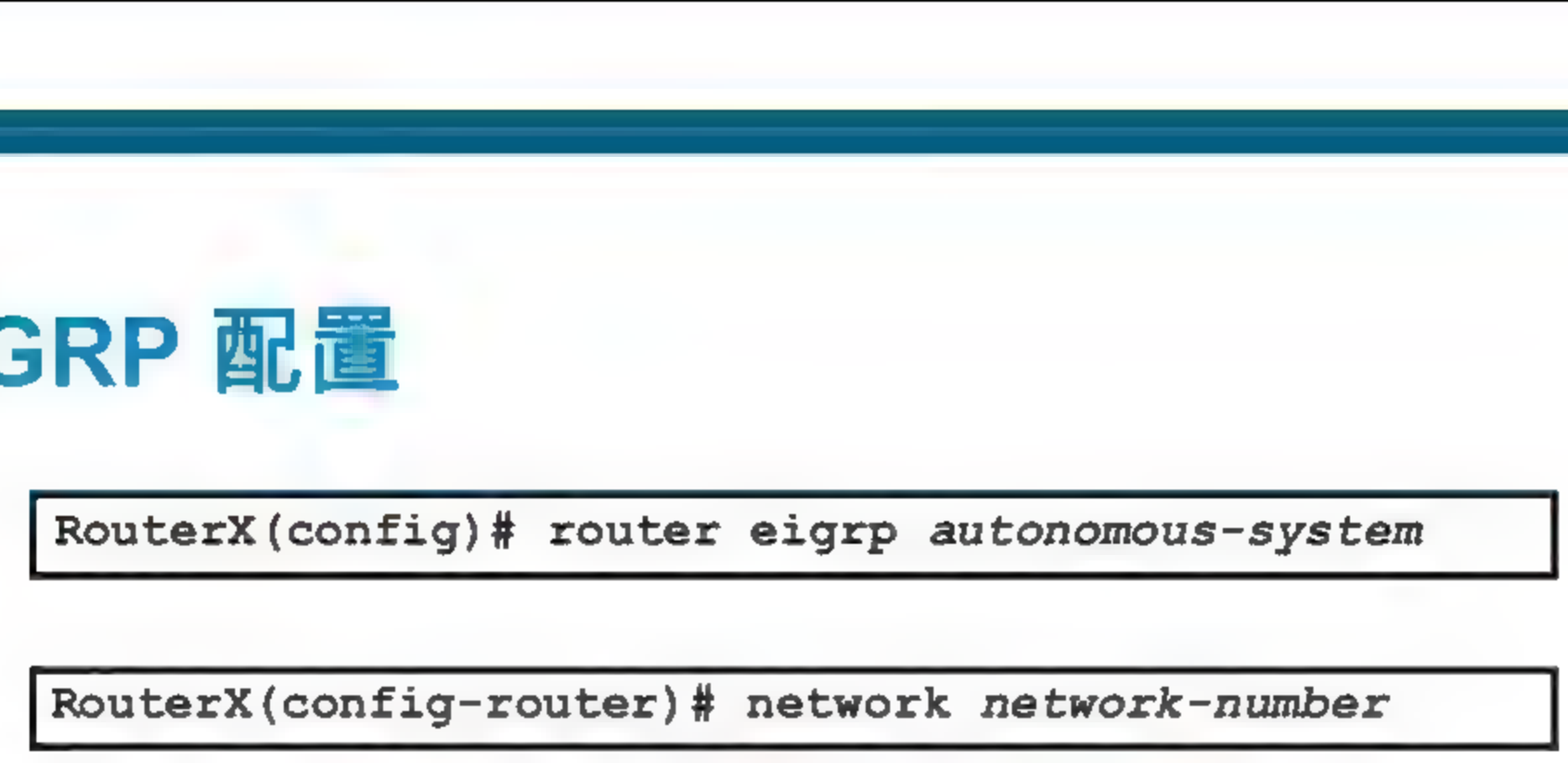
327P 095

© 2008 Cisco Systems, Inc. 保留所有权利。

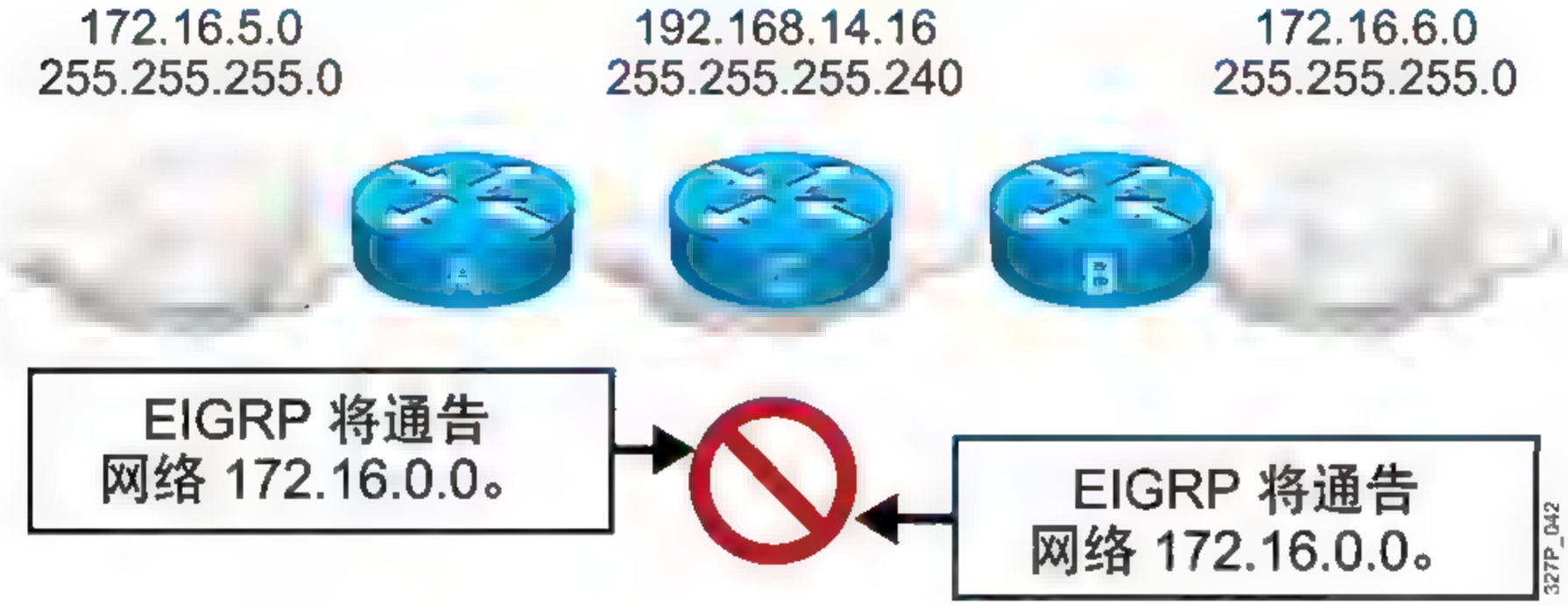
EIGRP 配置

```
RouterX(config)# router eigrp autonomous-system
```

```
RouterX(config-router)# network network-number
```

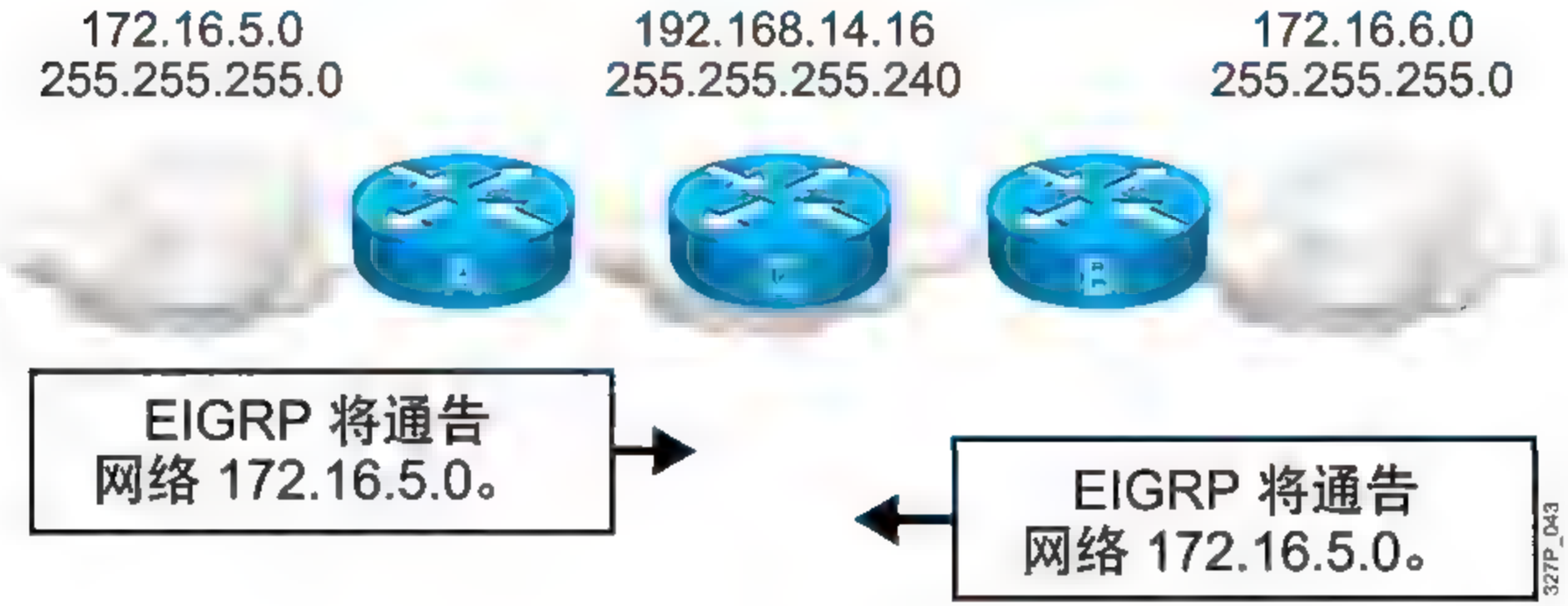


EIGRP 和不连续网络的默认场景配置



默认情况下，EIGRP 不通告子网，因此它不支持不连续子网。

具有 no auto-summary 命令的 EIGRP 和不连续网络



具有 **no auto-summary** 命令的 EIGRP 可通告子网，因此它能够支持不连续子网。

检验 EIGRP 配置

```
RouterX# show ip route eigrp
```

- 显示路由表中的当前 EIGRP 条目

```
RouterX# show ip protocols
```

- 显示活动进程的参数和当前状态

```
RouterX# show ip eigrp interfaces
```

- 显示为 EIGRP 配置的接口信息

```
RouterX# sh ip eigrp interfaces
IP-EIGRP interfaces for process 100
                      Xmit Queue     Mean   Pacing Time   Multicast    Pending
Int         Peers     Un/Reliable    SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0         0         0/0           0       0/1           0           0
Se0/0/0       1         0/0          38      10/380         552         0
```

检验 EIGRP 配置（续）

```
RouterX# show ip eigrp neighbors [detail]
```

- 显示 IP EIGRP 发现的邻居

```
RouterX# show ip eigrp neighbors
IP-EIGRP neighbors for process 77
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
2   172.16.1.14             Se3/0             11 00:00:44   52   2280  0  10
1   172.16.1.10             Se1/0             11 00:00:45   62   2022  0  7
0   10.1.1.1                Et0/0             10 00:00:49   14    200  0  2
```

检验 EIGRP 配置（续）

```
RouterX# show ip eigrp topology [all-links]
```

- 显示 IP EIGRP 拓扑表
- 不带 **[all-links]** 参数时，显示后继路由和可行的后续路由

```
RouterX# show ip eigrp topology
IP-EIGRP Topology Table for AS(77)/ID(172.16.1.13)

Codes:P - Passive, A - Active, U - Update, Q - Query, R - Reply,
    r - reply Status, s - sia Status

P 10.2.2.0/24, 1 successors, FD is 36092928
    via 172.16.1.10 (36092928/281600), Serial1/0
    via 172.16.1.14 (40537600/281600), Serial3/0
P 10.1.1.0/24, 1 successors, FD is 281600
    via Connected, Ethernet0/0
P 172.16.1.12/30, 1 successors, FD is 40512000
    via Connected, Serial3/0
P 172.16.1.8/30, 1 successors, FD is 36067328
    via Connected, Serial1/0
```

检验 EIGRP 配置（续）

```
RouterX# show ip eigrp traffic
```

- 显示发送和接收的 IP EIGRP 数据包数量

```
RouterX# show ip eigrp traffic
IP-EIGRP Traffic Statistics for AS 77
Hellos sent/received: 2882/2879
Updates sent/received: 20/10
Queries sent/received: 2/4
Replies sent/received: 4/2
Acks sent/received: 10/17
Input queue high water mark 2, 0 drops
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0
Hello Process ID: 84
PDM Process ID: 83
```

debug ip eigrp 命令

```
RouterX# debug ip eigrp
IP-EIGRP:Processing incoming UPDATE packet
IP-EIGRP:Ext 192.168.3.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 -
256000 104960
IP-EIGRP:Ext 192.168.0.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 -
256000 104960
IP-EIGRP:Ext 192.168.3.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 -
256000 104960
IP-EIGRP:172.69.43.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP:Ext 172.69.43.0 255.255.255.0 metric 371200 - 256000 115200
IP-EIGRP:192.135.246.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP:Ext 192.135.246.0 255.255.255.0 metric 46310656 - 45714176 596480
IP-EIGRP:172.69.40.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP:Ext 172.69.40.0 255.255.255.0 metric 2272256 - 1657856 614400
IP-EIGRP:192.135.245.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP:Ext 192.135.245.0 255.255.255.0 metric 40622080 - 40000000 622080
IP-EIGRP:192.135.244.0 255.255.255.0, - do advertise out Ethernet0/1
```

注：仅在拓扑结构变化时才交换 EIGRP 路由。

EIGRP 度量

EIGRP 默认用于计算其度量的标准：

- 带宽
- 延迟

EIGRP 可配置来用于计算其度量的可选标准：

- 可靠性
- 负载

注：虽然在邻居路由器间会通过 EIGRP 数据包交换 MTU 信息，但计算 EIGRP 度量时并未考虑 MTU 因素。

EIGRP 负载均衡

- 默认情况下，EIGRP 为等度量负载均衡：
  - 默认情况下，路由表中最多有四条路由的度量与最小度量相等。
- 路由表中的相同目的地最多可有 16 个条目：
  - 条目数量用 **maximum-paths** 命令来进行配置。

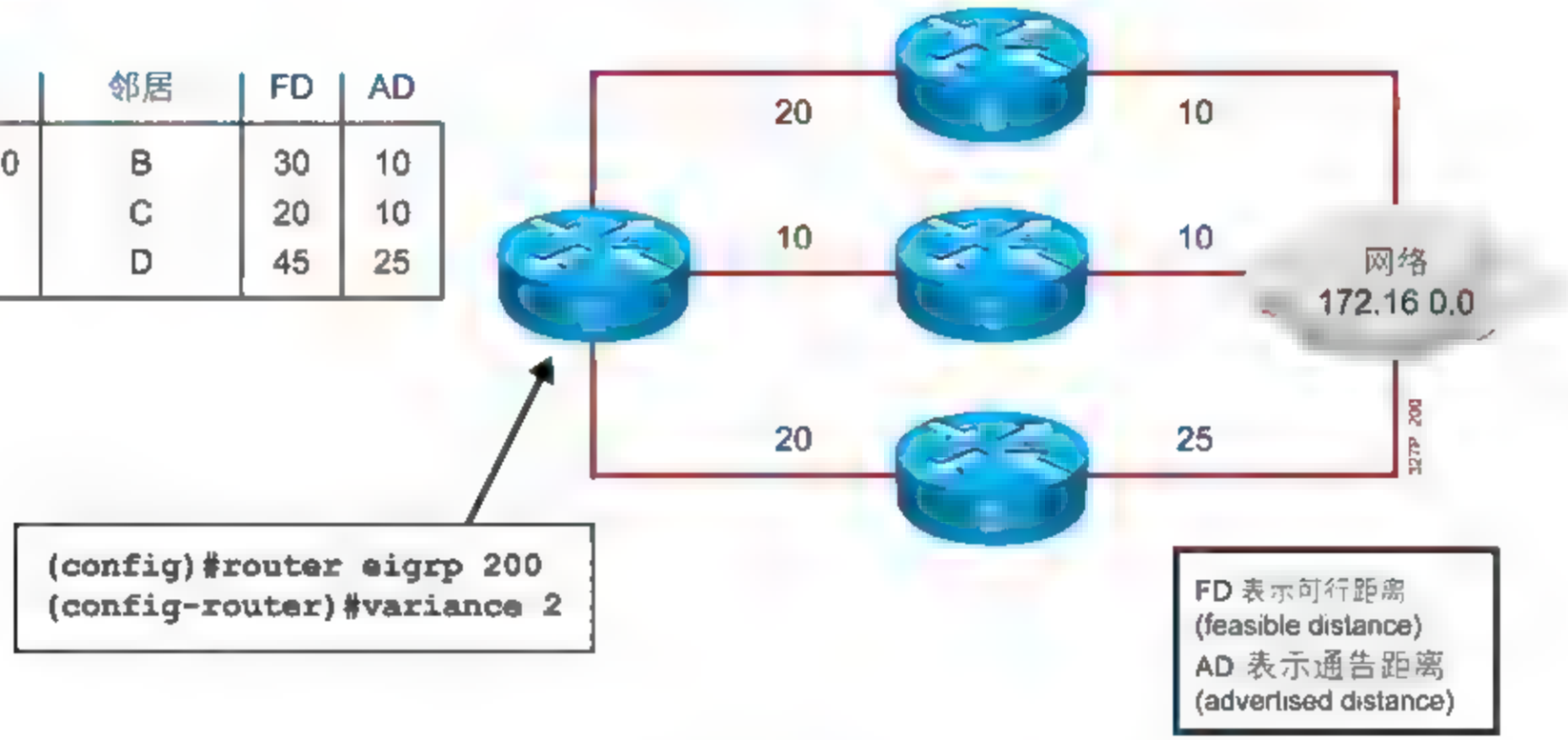
EIGRP 不等价负载均衡

```
RouterX(config-router)#
variance multiplier
```

- 允许路由器在路由度量小于 *multiplier* 值与路由到目的地的最小度量乘积的路由上实现负载均衡。
- 默认变量为 1，表示等价负载均衡。

变量示例

网络	邻居	FD	AD
172.16.0.0	B	30	10
	C	20	10
	D	45	25



- 因为路由器 C 的最短可行距离为 20，所以路由器 E 选择路由器 C 来路由到网络 172.16.0.0。
- 变量为 2 时，路由器 E 也选择路由器 B 来路由到网络 172.16.0.0，原因是 (20 + 10 = 30) < [2 * (FD) = 40]。
- 因为 25 > 20，所以不考虑用路由器 D 来路由到网络 172.16.0.0。

EIGRP MD5 身份验证

- EIGRP 支持 MD5 身份验证。
- 路由器对每个它发送的 EIGRP 数据包进行自我标识。
- 路由器验证接收到的每个路由更新数据包的来源。
- 每个参与的邻居都必须配置相同的密钥。

EIGRP MD5 身份验证配置步骤

1. 创建密钥链，它是一组可能的密钥（密码）。
2. 对每个密钥分配密钥 ID。
3. 标识密钥。
4. （可选）指定密钥的有效期。
5. 在接口上启用 MD5 身份验证。
6. 指定接口使用的密钥链。

配置 EIGRP MD5 身份验证

```
RouterX(config)#
key chain name-of-chain
```

- 进入密钥链配置模式

```
RouterX(config-keychain)#
key key-id
```

- 标识密钥并进入密钥 ID 的配置模式

配置 EIGRP MD5 身份验证（续）

```
RouterX(config-keychain-key)#
```

```
key-string text
```

- 标识密钥字符串（密码）

```
RouterX(config-keychain-key)#
```

```
accept-lifetime start-time {infinite | end-time | duration
seconds}
```

- （可选）指定何时为收到的数据包接受密钥

```
RouterX(config-keychain-key)#
```

```
send-lifetime start-time {infinite | end-time | duration
seconds}
```

- （可选）指定密钥何时可用于发送数据包

配置 EIGRP MD5 身份验证（续）

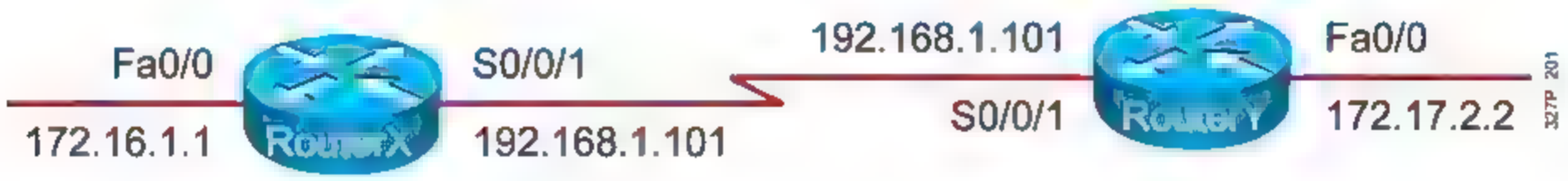
```
RouterX(config-if)#
ip authentication mode eigrp autonomous-system md5
```

- 为 EIGRP 数据包指定 MD5 身份验证

```
RouterX(config-if)#
ip authentication key-chain eigrp autonomous-system
name-of-chain
```

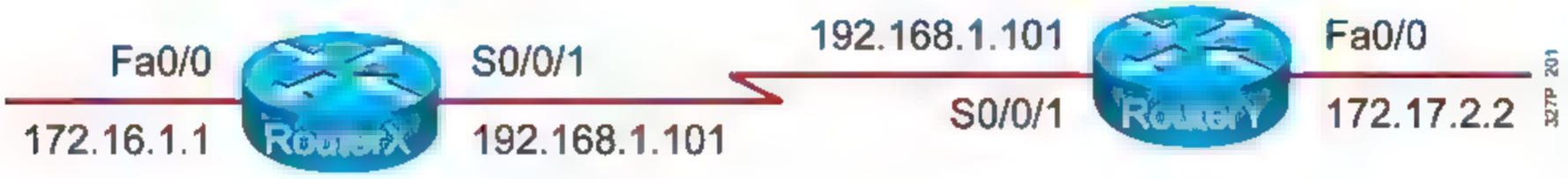
- 使用密钥链中的密钥来启用 EIGRP 数据包的身份验证

EIGRP MD5 身份验证配置示例




```
RouterX
<省略部分输出>
key chain RouterXchain
key 1
key-string firstkey
accept-lifetime 04:00:00 Jan 1 2006 infinite
send-lifetime 04:00:00 Jan 1 2006 04:01:00 Jan 1 2006
key 2
key-string secondkey
accept-lifetime 04:00:00 Jan 1 2006 infinite
send-lifetime 04:00:00 Jan 1 2006 infinite
<省略部分输出>
!
interface Serial0/0/1
bandwidth 64
ip address 192.168.1.101 255.255.255.224
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 RouterXchain
```

EIGRP MD5 身份验证配置示例（续）

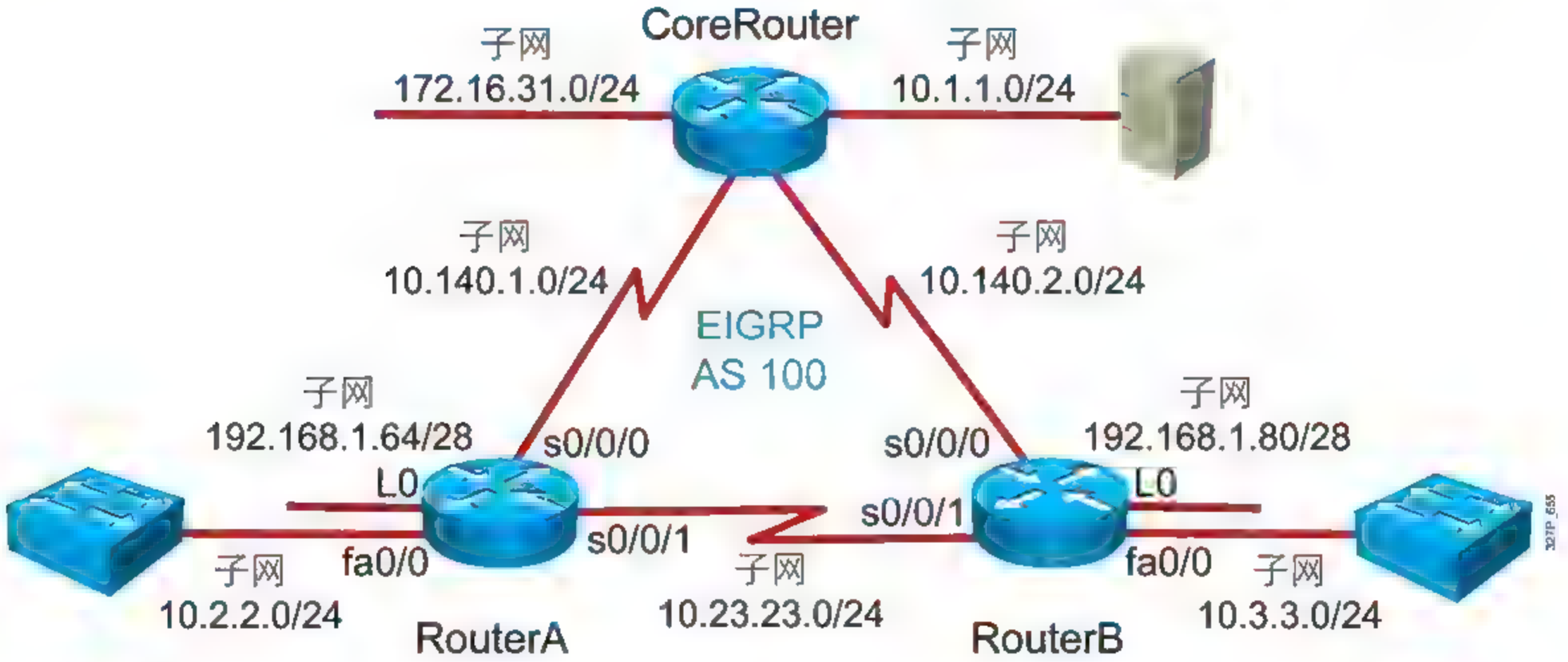



```
RouterY
<省略部分输出>
key chain RouterYchain
key 1
key-string firstkey
accept-lifetime 04:00:00 Jan 1 2006 infinite
send-lifetime 04:00:00 Jan 1 2006 infinite
key 2
key-string secondkey
accept-lifetime 04:00:00 Jan 1 2006 infinite
send-lifetime 04:00:00 Jan 1 2006 infinite
<省略部分输出>
!
interface Serial0/0/1
bandwidth 64
ip address 192.168.1.102 255.255.255.224
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 RouterYchain
```

检验 MD5 身份验证

```
RouterX#
*Jan 21 16:23:30.517:%DUAL-5-NBRCHANGE:IP-EIGRP(0) 100:Neighbor 192.168.1.102
(Serial0/0/1) is up:new adjacency

RouterX# show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                            (sec)             (ms)       Cnt Num
0   192.168.1.102           Se0/0/1          12 00:03:10    17   2280  0  14

RouterX# show ip route
<省略部分输出>
Gateway of last resort is not set
D    172.17.0.0/16 [90/40514560] via 192.168.1.102, 00:02:22, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:31:31, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.96/27 is directly connected, Serial0/0/1
D       192.168.1.0/24 is a summary, 00:31:31, Null0

RouterX#ping 172.17.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/15/16 ms
```

可视目标 5-1：实施 EIGRP



总结

- EIGRP 是运行 DUAL 算法的无类高级距离矢量路由协议。
- EIGRP 要求您配置的自治系统编号必须与所有路由器匹配才能交换路由。
- EIGRP 能够在不等价路径上实现负载均衡。
- EIGRP 支持 MD5 身份验证以防止未授权的非法路由器进入网络。

CISCO

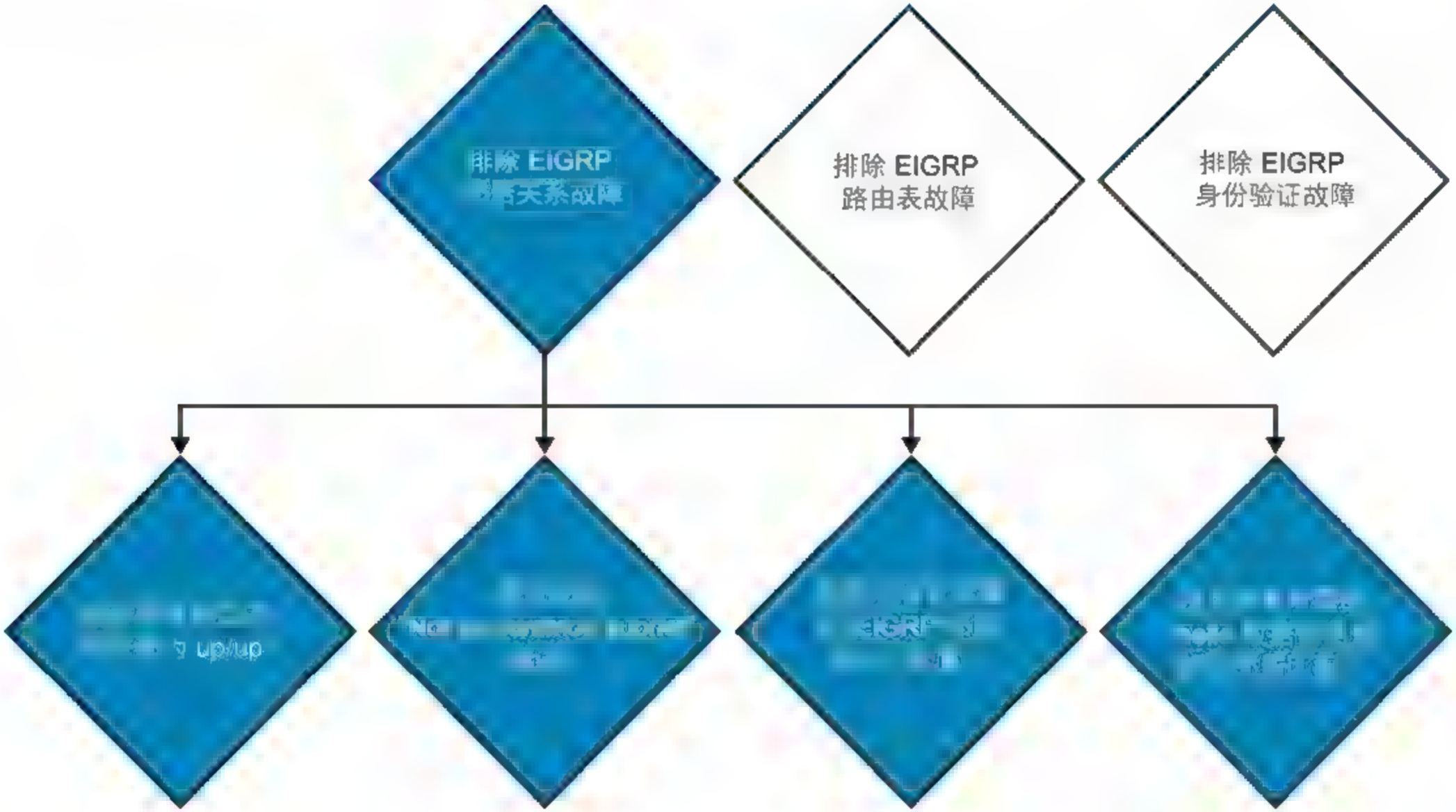
EIGRP 故障排除

EIGRP 实施

EIGRP 故障排除的组成部分

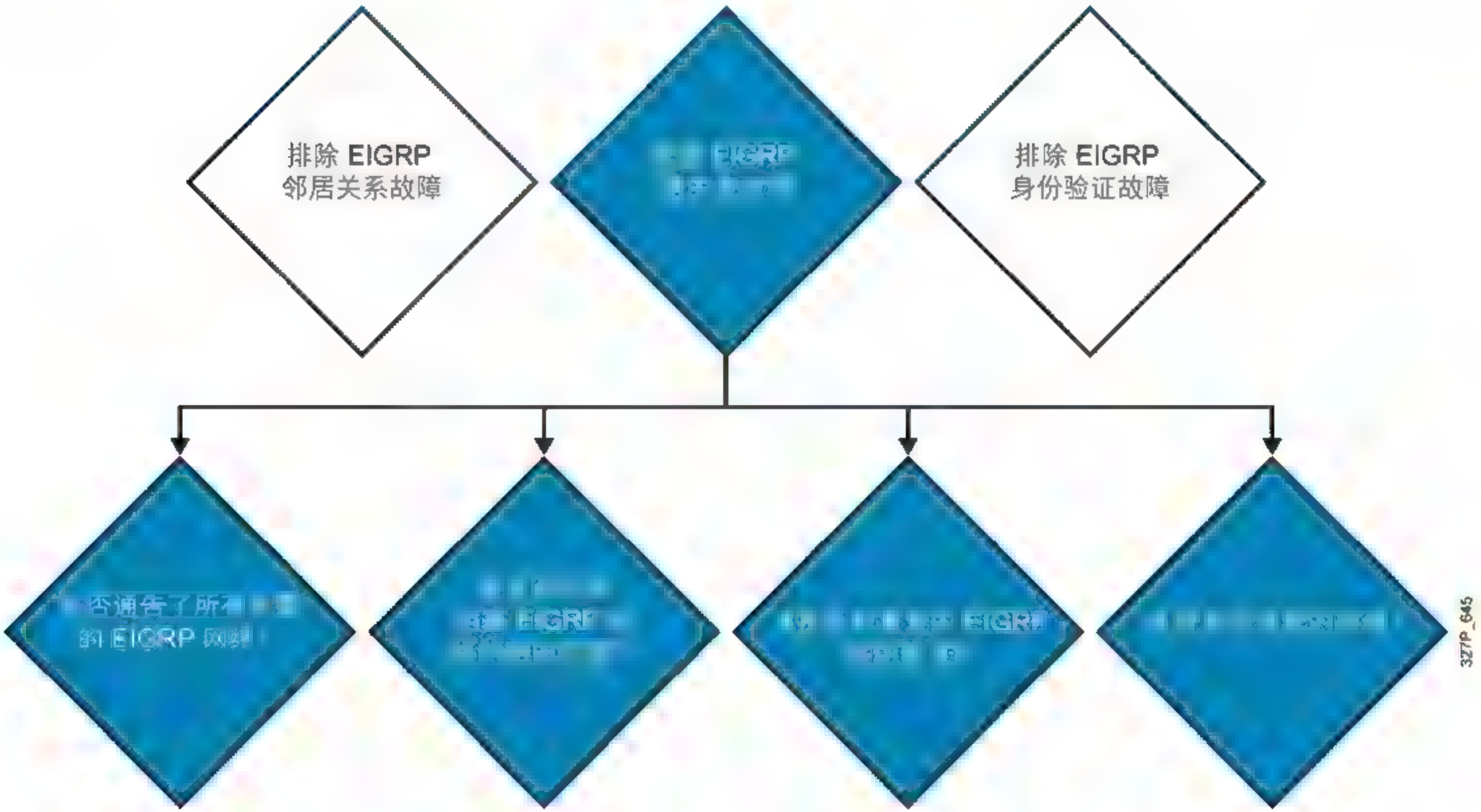
© 2008 Cisco Systems, Inc. 保留所有权利。

EIGRP 邻居问题的故障排除



© 2008 Cisco Systems, Inc. 保留所有权利。

EIGRP 路由表故障排除



© 2008 Cisco Systems, Inc. 保留所有权利。

EIGRP 身份验证故障排除

RouterX 与 RouterY 之间成功的 MD5 身份验证

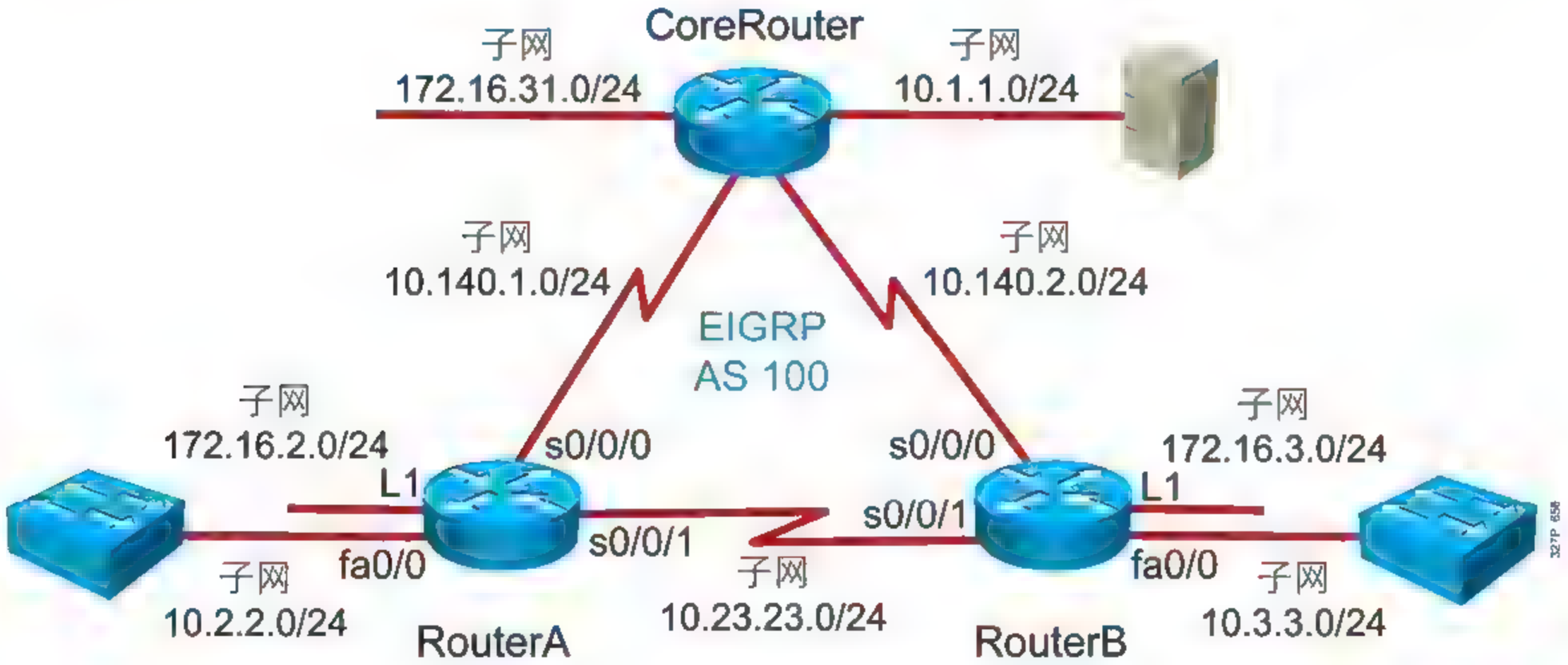
```
RouterX# debug eigrp packets
EIGRP Packets debugging is on
  (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)
*Jan 21 16:38:51.745:EIGRP:received packet with MD5 authentication, key id = 1
*Jan 21 16:38:51.745:EIGRP:Received HELLO on Serial0/0/1 nbr 192.168.1.102
*Jan 21 16:38:51.745:AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 pe
erQ un/rely 0/0

RouterY# debug eigrp packets
EIGRP Packets debugging is on
(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY,
SIAREPLY)
RouterY#
*Jan 21 16:38:38.321:EIGRP:received packet with MD5 authentication, key id = 2
*Jan 21 16:38:38.321:EIGRP:Received HELLO on Serial0/0/1 nbr 192.168.1.101
*Jan 21 16:38:38.321:AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 pe
erQ un/rely 0/0
```

排除 EIGRP 身份验证问题

RouterX 的密钥 2 改变时，RouterX 与 RouterY 之间 MD5 身份验证不成功

```
RouterX(config-if)#key chain RouterXchain
RouterX(config-keychain)#key 2
RouterX(config-keychain-key)#key-string wrongkey

RouterY#debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)
RouterY#
*Jan 21 16:50:18.749: EIGRP: pkt key id = 2, authentication mismatch
*Jan 21 16:50:18.749: EIGRP: Serial0/0/1: ignored packet from 192.168.1.101, opc
ode = 5 (invalid authentication)
*Jan 21 16:50:18.749: EIGRP: Dropping peer, invalid authentication
*Jan 21 16:50:18.749: EIGRP: Sending HELLO on Serial0/0/1
*Jan 21 16:50:18.749:   AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
*Jan 21 16:50:18.753: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.1.101
 (Serial0/0/1) is down: Auth failure

RouterY#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
RouterY#
```

可视目标 5-2：
EIGRP 故障排除



总结

- EIGRP 的故障排除涉及几个方面，例如解决邻居关系问题、路由表问题和身份验证问题。
- 导致 EIGRP 邻居问题的原因包括错误的网络命令和 hello 数据包信息不匹配。使用 **show ip eigrp neighbors** 命令有助于排除这些问题。
- 路由表中丢失 EIGRP 路由的原因可能是路由过滤或不连续网络中的自动总结。使用 **show ip route** 命令有助于排除这些问题。
- **degub eigrp packets** 命令可帮助您排除 MD5 身份验证问题。

CISCO

单元总结

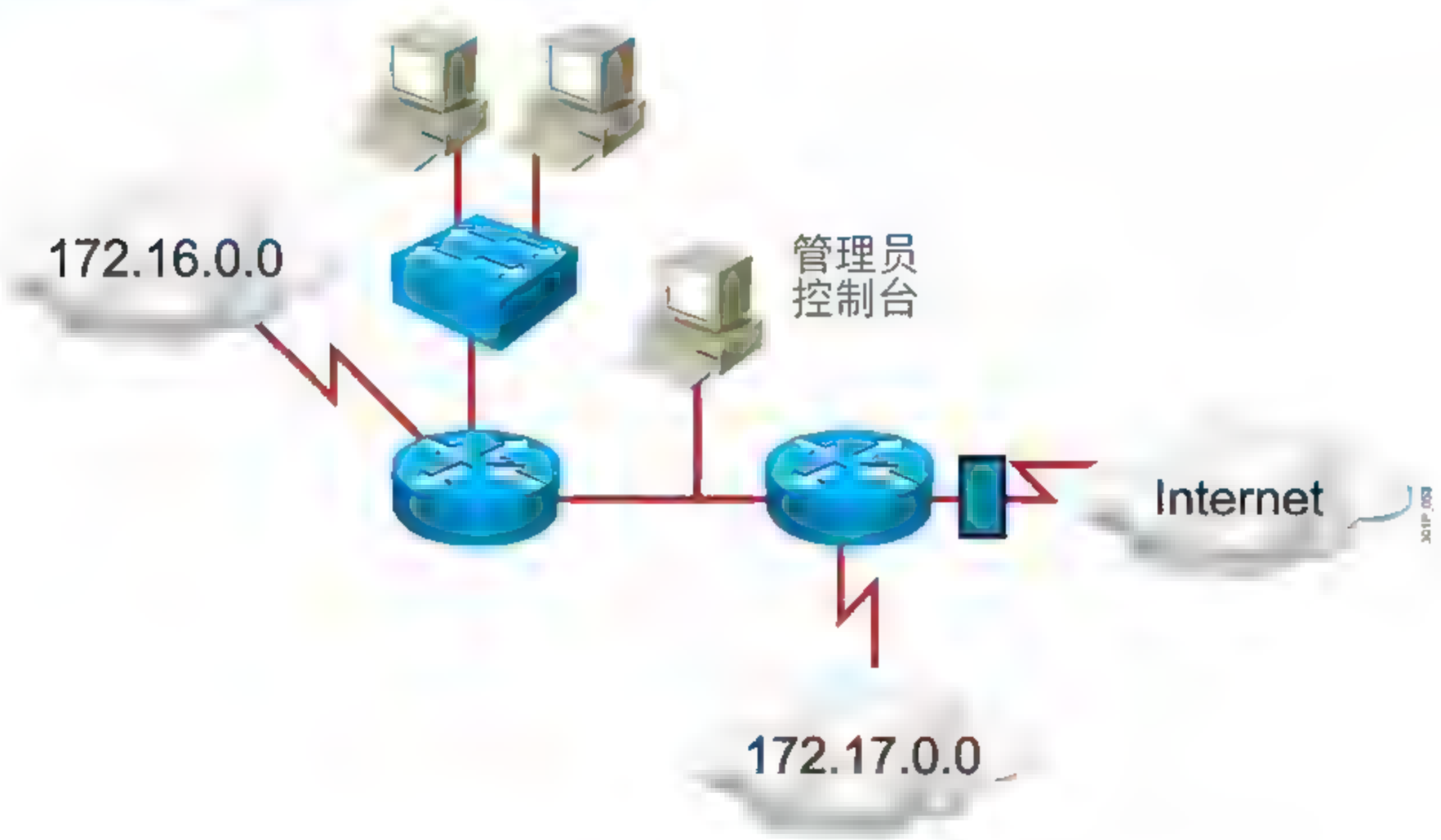
- EIGRP 是支持 VLSM 的无类路由协议。
- 路径选择取决于几个因素。
- EIGRP 保留下一个最佳备用路径（称为可行后继路由）用于快速收敛。
- EIGRP 支持不等价负载均衡。
- EIGRP 使用 MD5 身份验证来验证路由器的真实性。
- EIGRP 的故障排除需要解决链路、邻居、重分布和路由问题。
- 以下命令能帮助您排除 EIGRP 问题：**show ip eigrp neighbor**、**show ip eigrp topology**、**show ip eigrp interface** 和 **show ip route**。

CISCO

ACL 运行简介

访问控制列表

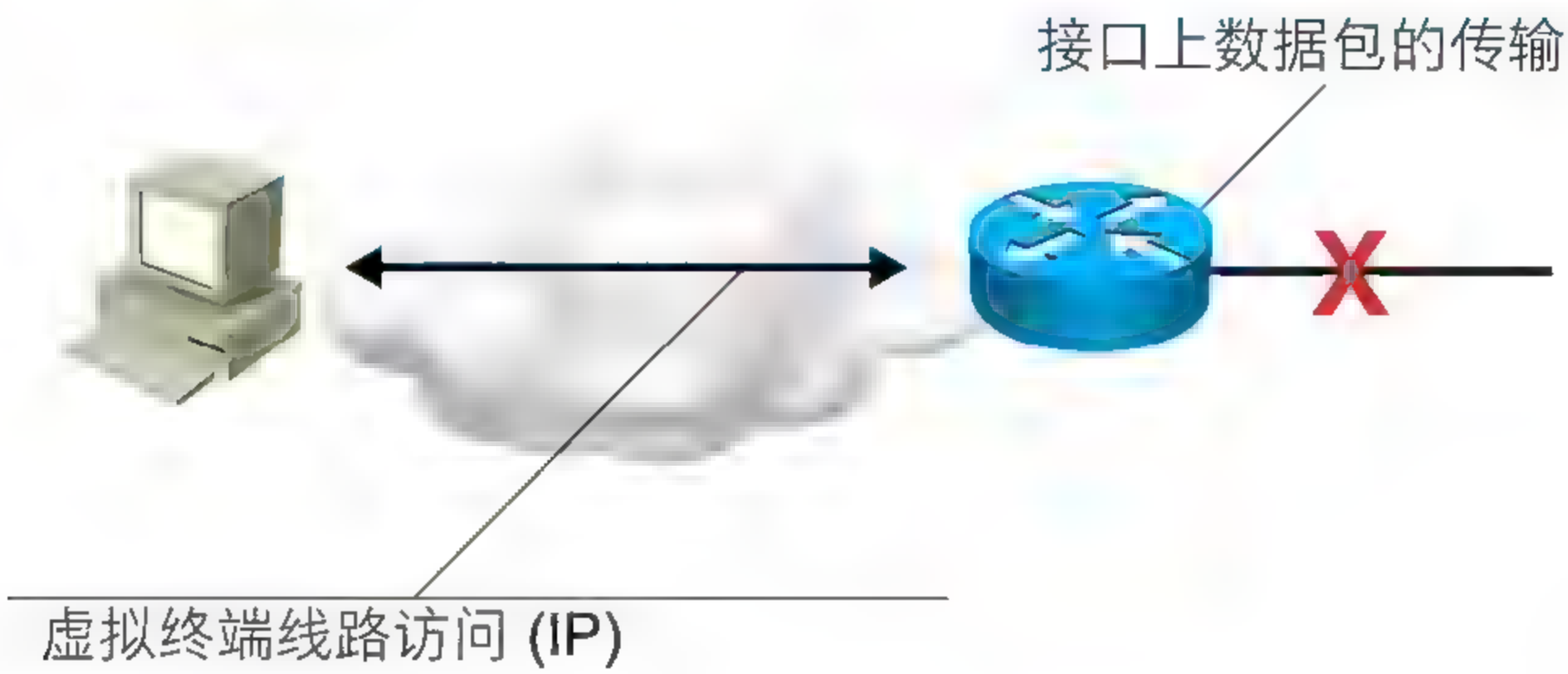
为什么要使用 ACL？



- 过滤：通过过滤经过路由器的数据包来管理 IP 流量
- 分类：标识流量以进行特殊处理

stems Inc. 保留所有权利。

ACL 的应用：过滤



301P 054

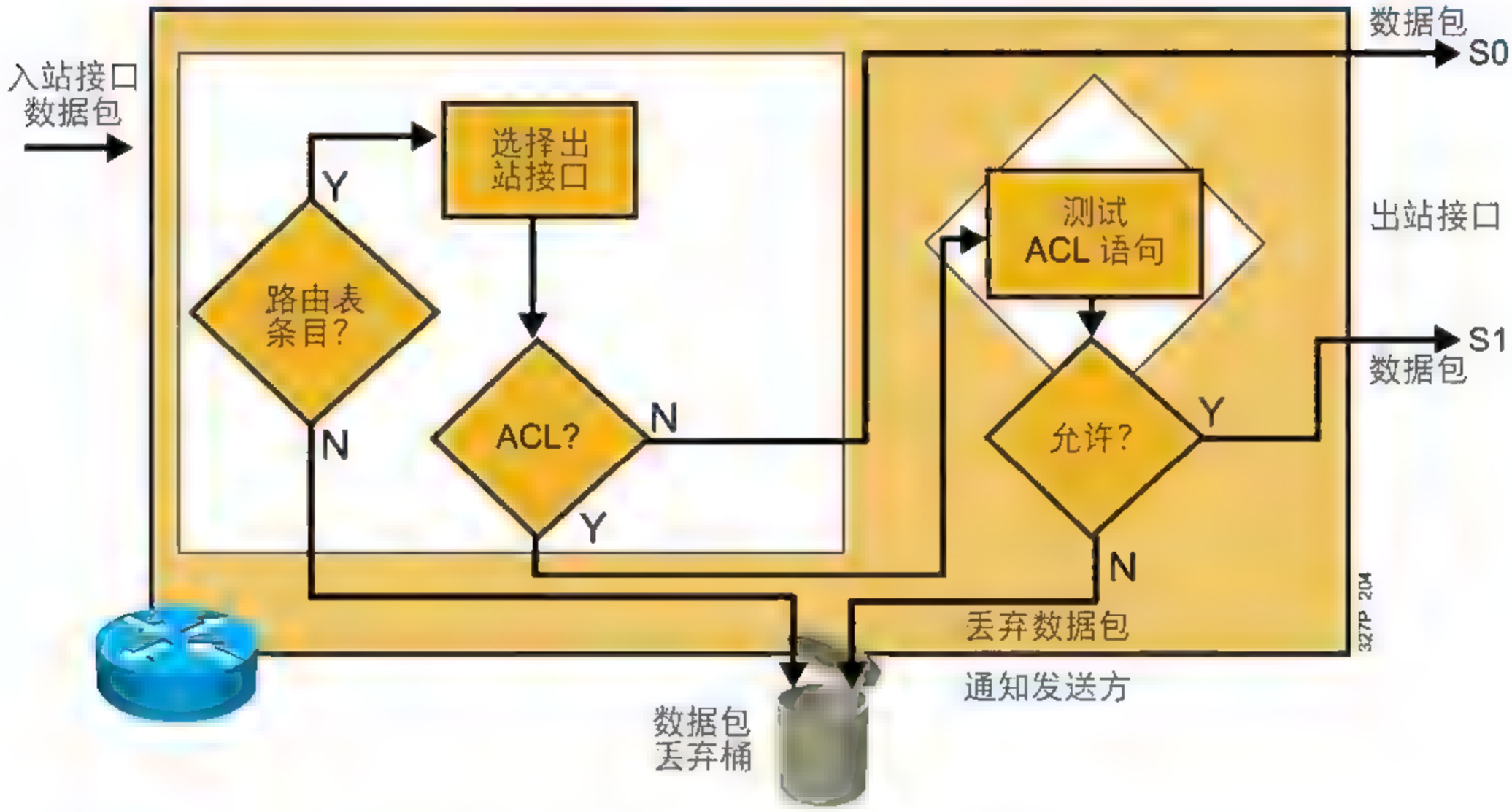
- 允许或拒绝经过路由器的数据包。
- 允许或拒绝来自路由器或到路由器的 vty 访问。
- 如果没有 ACL，所有数据包会发往网络的所有部分。

ACL 的应用：分类

根据数据包测试情况对流量进行特殊处理

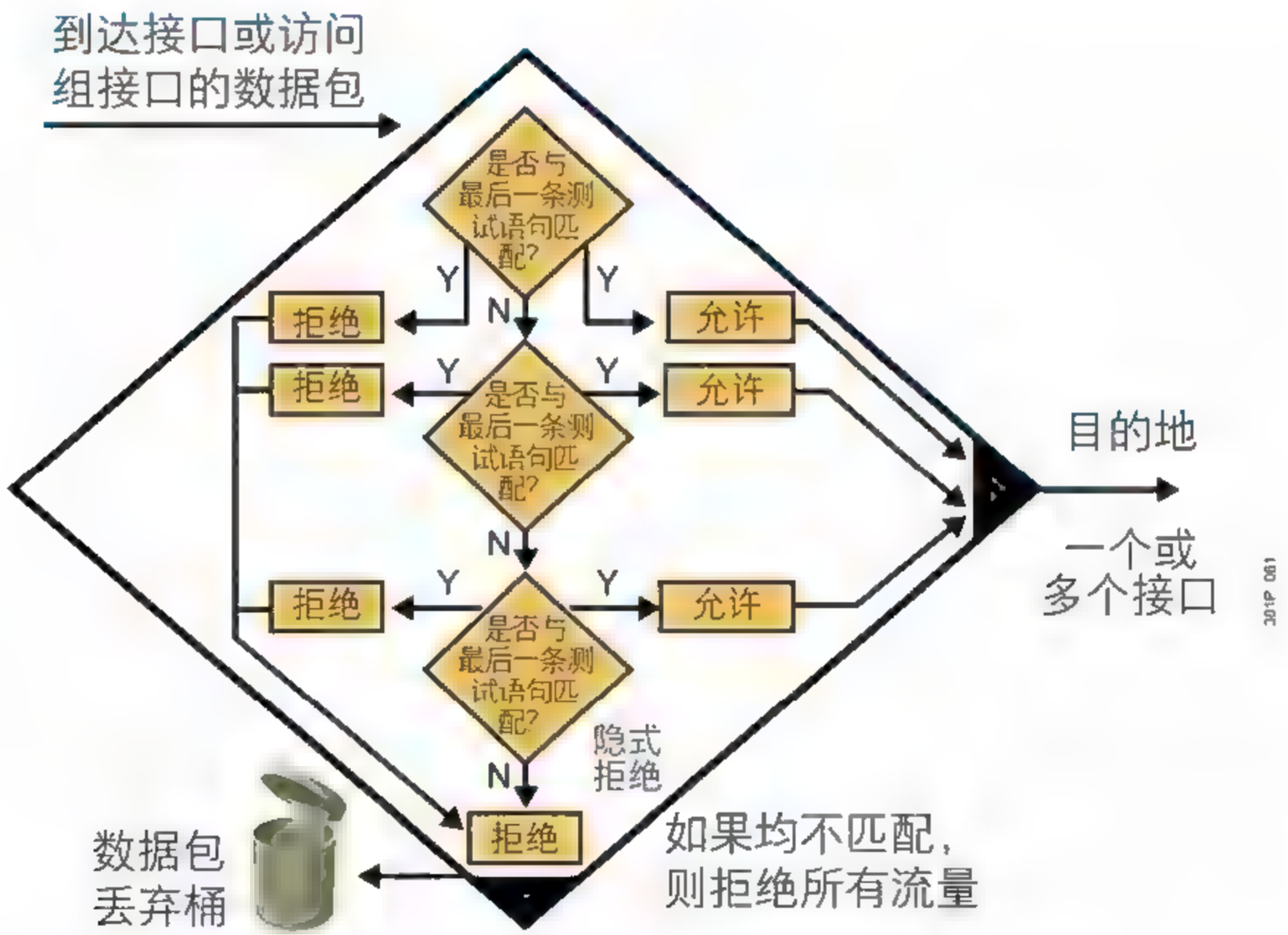
© 2016 Cisco Systems, Inc. 保留所有权利。

出站 ACL 运行



如果没有 ACL 语句匹配，则丢弃数据包。

测试步骤：拒绝或允许


到达接口或访问
组接口的数据包
是否与
最后一条测
试语句匹
配?
Y
N
拒绝
允许
是否与
最后一条测
试语句匹
配?
是否与
最后一条测
试语句匹
配?
隐式
拒绝
拒绝
目的地
一个或
多个接口
数据包
丢弃桶
如果均不匹配，
则拒绝所有流量

ACL 的类型

- 标准 ACL
  - 检查源地址
  - 通常允许或拒绝整个协议簇
- 扩展 ACL
  - 检查源地址和目的地址
  - 通常允许或拒绝特定协议和应用程序
- 有两种用于标识
标准 ACL 和扩展 ACL 的方法：
  - 编号 ACL 使用编号进行标识
  - 命名 ACL 使用描述性名称或编号进行标识

如何标识 ACL

IPv4 ACL 类型	编号范围/标识符
采用数字编号的标准 ACL、采用数字编号的扩展 ACL、命名 ACL（标准和扩展）	1–99, 1300–1999 100–199, 2000–2699 名称

327P_515

- 标准编号 IPv4 列表 (1-99) 可测试源地址的所有 IP 数据包的条件。扩展范围是 (1300-1999)。
- 扩展编号 IPv4 列表 (100-199) 可测试源地址和目的地址、特定 TCP/IP 协议和目的端口的条件。扩展范围是 (2000-2699)。
- 命名 ACL 用字母数字字符串（名称）标识 IP 标准 ACL 和扩展 ACL。

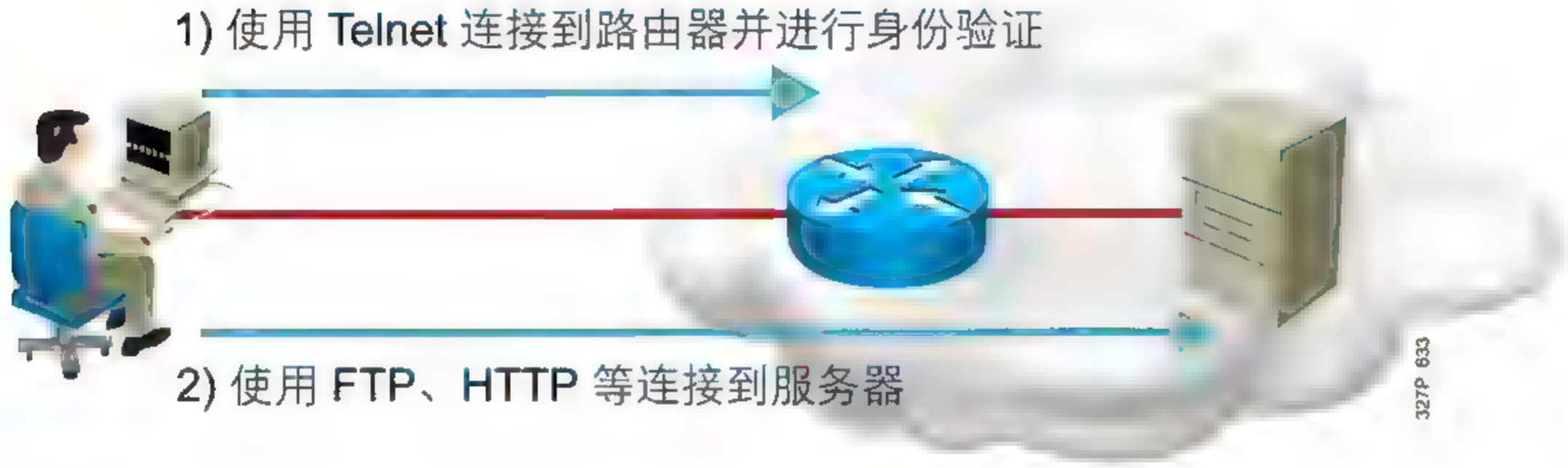
IP 访问列表条目序列编号

- 需要 Cisco IOS 12.3 版
- 允许使用序列编号来编辑 ACL 语句的顺序
  - 在 Cisco IOS 12.3 版之前，使用文本编辑器来创建 ACL 语句，然后将语句以正确的顺序复制到路由器中。
- 允许使用序列号从列表中删除单条 ACL 语句
  - 在 Cisco IOS 12.3 版之前的软件中使用命名 ACL 时，必须使用 **no {deny | permit} protocol source source-wildcard destination destination-wildcard** 来删除单条语句。
  - 在 Cisco IOS 12.3 版之前的软件中使用编号 ACL 时，必须删除整个 ACL 才能删除单条 ACL 语句。

ACL 配置的指导原则

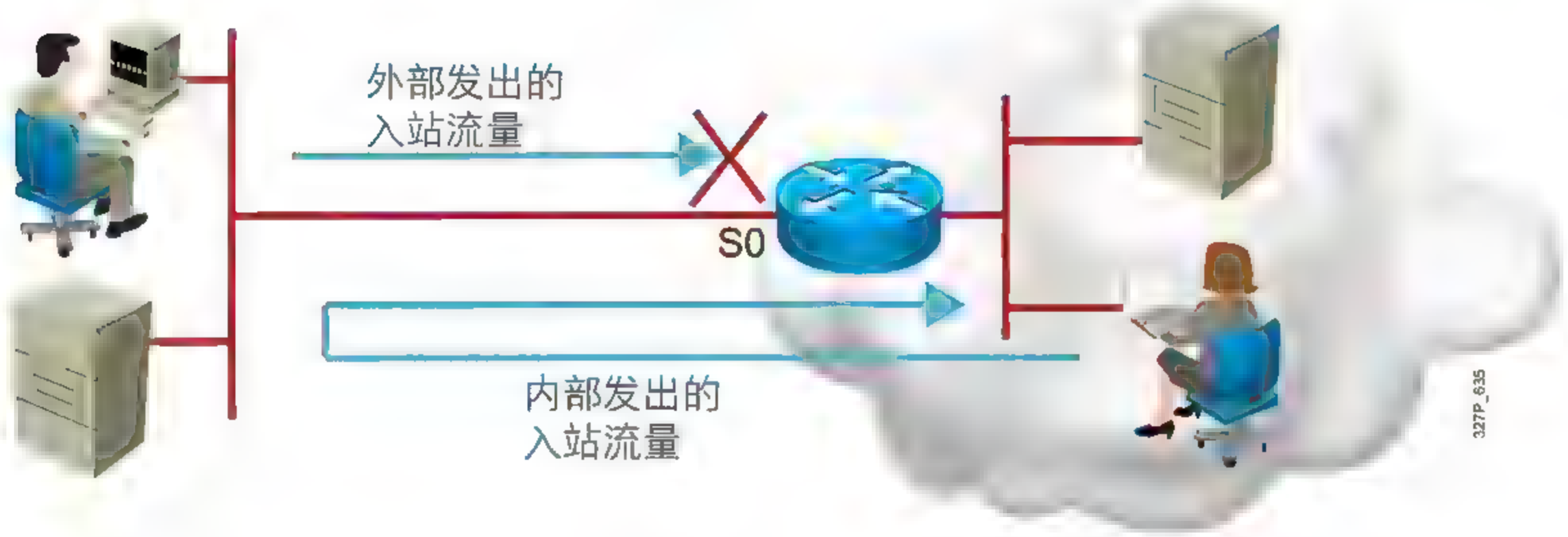
- 标准或扩展代表可过滤的内容。
- 每个接口、协议、方向只允许有一个 ACL。
- ACL 语句的顺序控制着测试，因此最具体的语句位于列表顶部。
- 最后的 ACL 测试始终是隐式拒绝其它所有语句，因此每个列表需要至少一条 permit 语句。
- 在全局范围内创建 ACL，然后将其应用到入站流量或出站流量的接口。
- ACL 可过滤经过路由器的流量或往返路由器的流量，具体取决于其应用方式。
- 将 ACL 置于网络中时：
  - 扩展 ACL 应靠近源地址
  - 标准 ACL 应靠近目的地址

动态 ACL



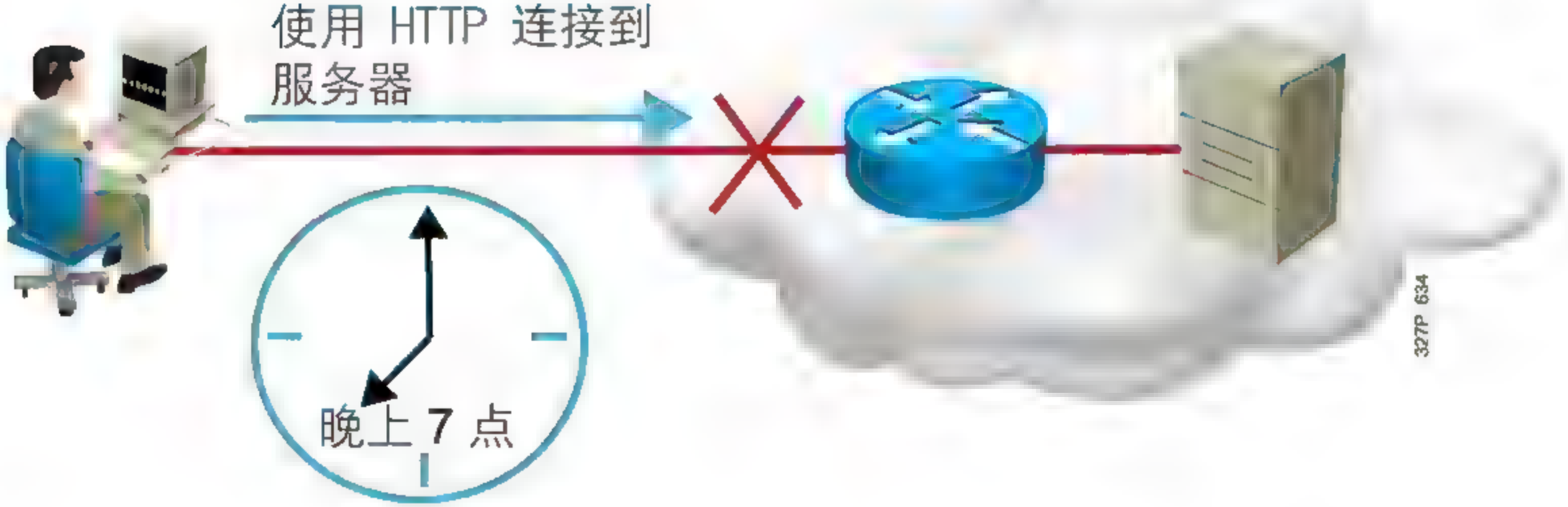
动态 ACL（锁和钥匙）：想要穿越路由器的用户需要使用 Telnet 来连接路由器并通过身份验证，否则将会被拦截。

自反 ACL



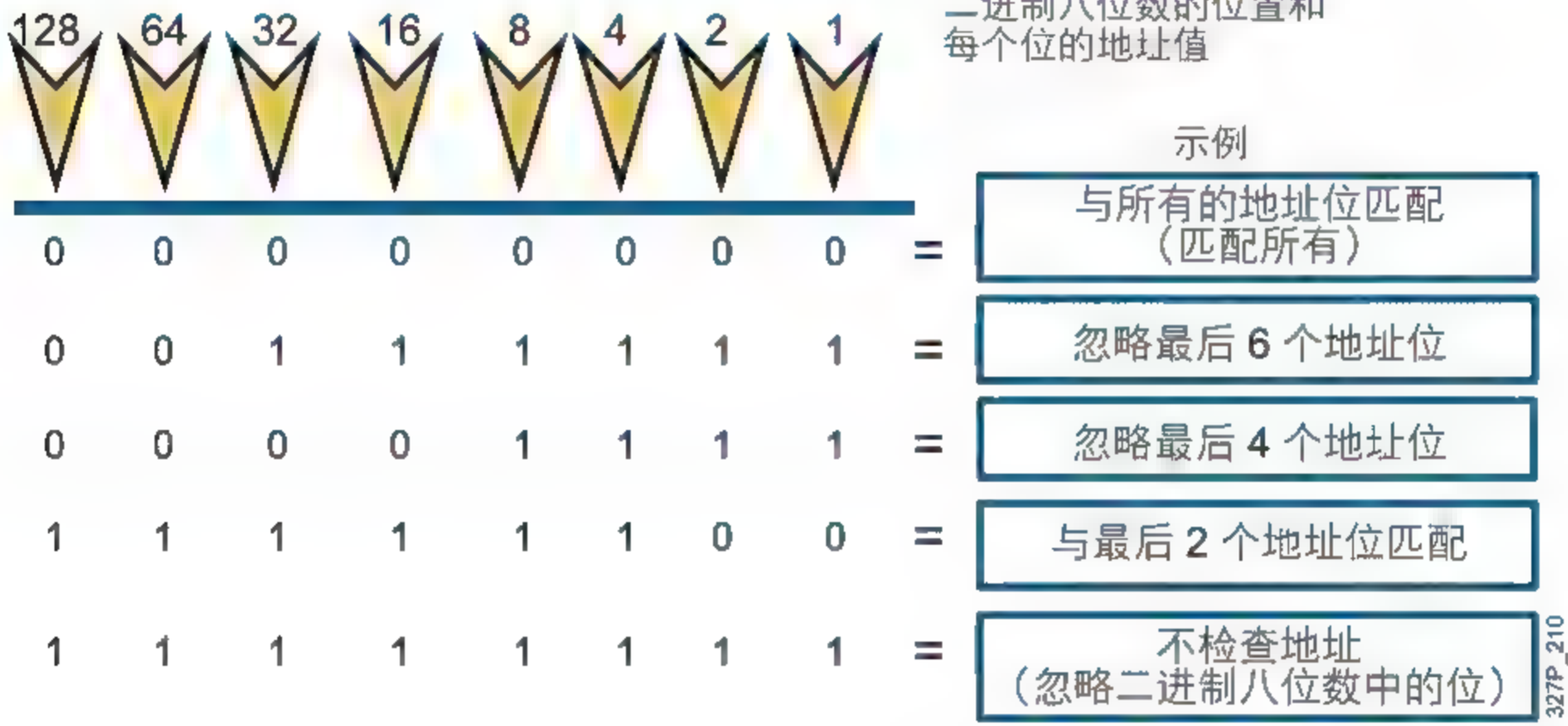
自反 ACL：用于允许出站流量并限制入站流量，以响应来自路由器内部的会话

基于时间的 ACL



基于时间的 ACL：允许根据天数和周数控制访问

通配符位：如何检查对应的地址位



- 0 表示匹配对应地址位的值
- 1 表示忽略对应地址位的值

用通配符位匹配 IP 子网

匹配 IP 子网 172.30.16.0/24 至 172.30.31.0/24。

地址和通配符掩码：

172.30.16.0 0.0.15.255

网络.主机

172.30.16.0

通配符掩码:

	0	0	0	1	0	0	0	0	
	0	0	0	0	1	1	1	1	
	|<---	匹配	----	>|<	---	忽略	---->|	
	0	0	0	1	0	0	0	0	= 16
	0	0	0	1	0	0	0	1	= 17
	0	0	0	1	0	0	1	0	= 18
					:				:
	0	0	0	1	1	1	1	1	= 31

327P 514

通配符位掩码的缩写

- 172.30.16.29 0.0.0.0 匹配所有地址位
- 使用前面有关键字 **host** 的 IP 地址 (host 172.30.16.29) 来缩写此通配符掩码

- 0.0.0.0 255.255.255.255 忽略所有地址位
- 用关键字 **any** 缩写表达式

327P_211

总结

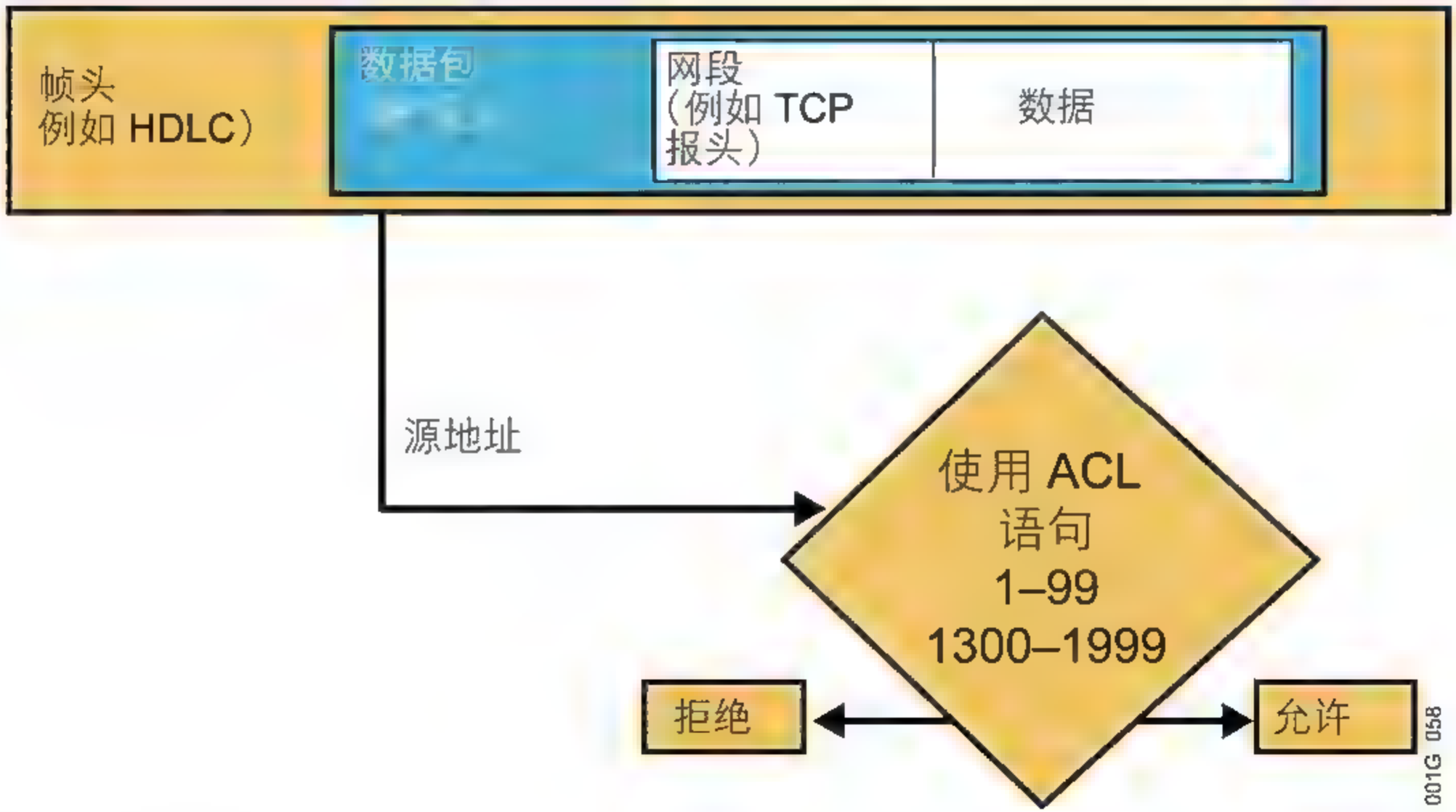
- ACL 可用于 IP 数据包过滤或标识流量以将其分配给特殊处理。
- ACL 执行自上而下的过程，并可针对入站或出站流量进行配置。
- 可使用命名 ACL 或编号 ACL 来创建 ACL。命名 ACL 或编号 ACL 可配置为标准 ACL 或扩展 ACL，以确定过滤的内容。
- 自反、动态和基于时间的 ACL 为标准 ACL 和扩展 ACL 增加了更多功能。
- 在通配符位掩码中，0 位表示匹配对应地址位，1 位表示忽略对应地址位。

CISCO

ACL 配置与故障排除

访问控制列表

用标准编号 IPv4 ACL 测试数据包



标准编号 IPv4 ACL 的配置

RouterX(config)#

```
access-list access-list-number
{permit | deny | remark} source [mask]
```

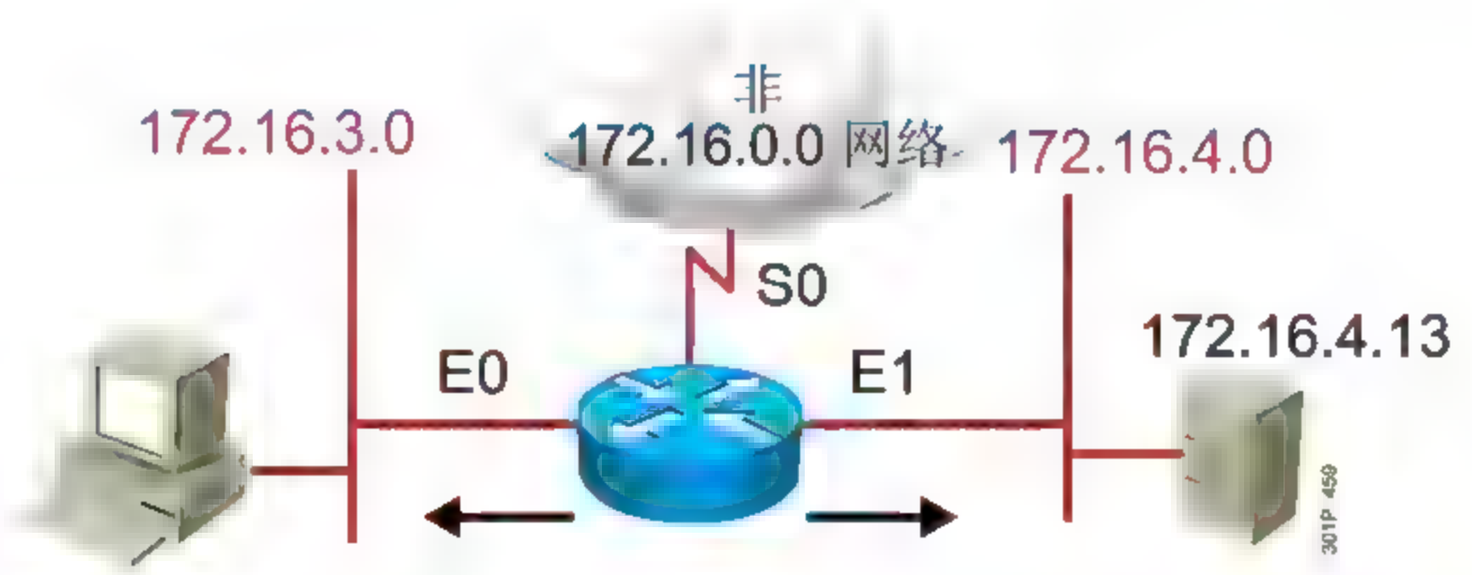
- 使用 1 到 99 或 1300 到 1999 作为*access-list-number*。
- 第一个条目分配的序列号是 10，
  后续条目以 10 为增量递增。
- 默认通配符掩码是 0.0.0.0（仅针对标准 ACL）。
- **no access-list access-list-number** 命令可删除整个 ACL。
- **remark** 用于向 ACL 添加说明。

RouterX(config-if)#

```
ip access-group access-list-number  {in | out}
```

- 激活接口上的列表。
- 设置入站或出站测试。
- **no ip access-group access-list-number {in | out}** 命令可从接口删除 ACL。

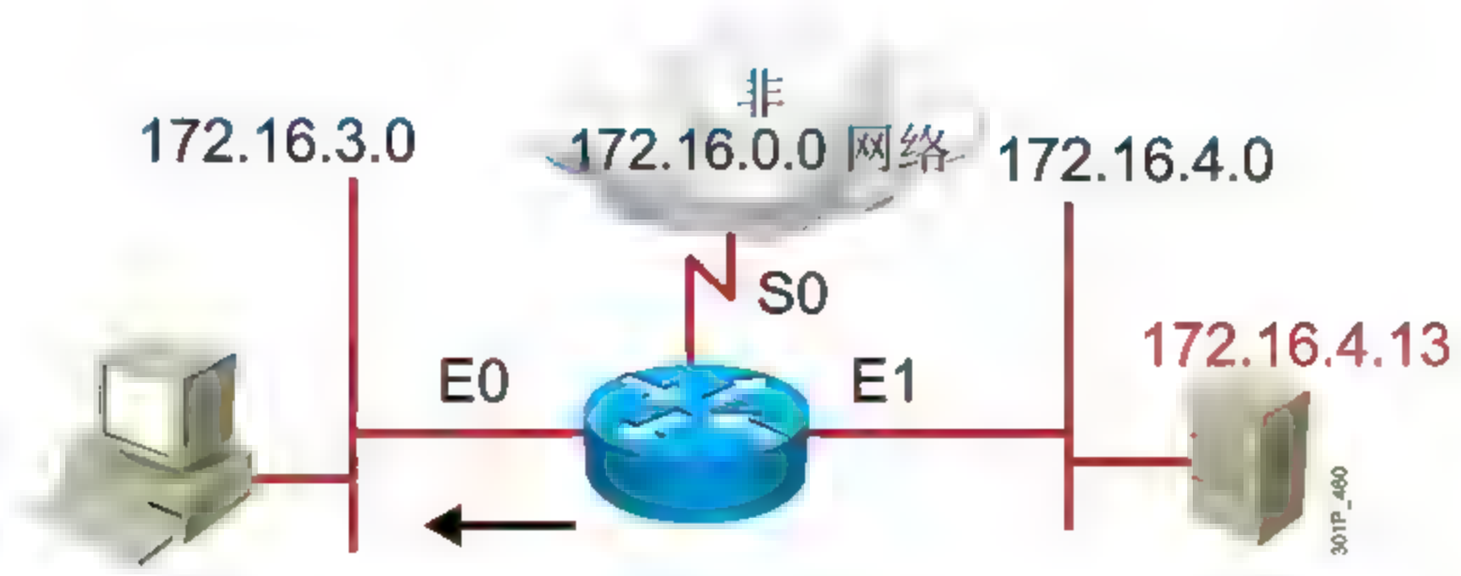
标准编号 IPv4 ACL 示例 1




```
RouterX(config)# access-list 1 permit 172.16.0.0  0.0.255.255
(隐式拒绝所有 – 在列表中不可见)
(access-list 1 deny 0.0.0.0   255.255.255.255)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 1 out
RouterX(config)# interface ethernet 1
RouterX(config-if)# ip access-group 1 out
```

仅允许我的网络

标准编号 IPv4 ACL 示例 2




```
RouterX(config)# access-list 1 deny 172.16.4.13 0.0.0.0
RouterX(config)# access-list 1 permit 0.0.0.0  255.255.255.255
（隐式拒绝所有）
(access-list 1 deny 0.0.0.0   255.255.255.255)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 1 out
```

拒绝特定主机

标准编号 IPv4 ACL 示例 3

```
RouterX(config)# access-list 1 deny 172.16.4.0  0.0.0.255
RouterX(config)# access-list 1 permit any
（隐式拒绝所有）
(access-list 1 deny 0.0.0.0   255.255.255.255)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 1 out
```

拒绝特定子网

用标准 ACL 控制 vty 访问

```
RouterX(config-line)#
access-class access-list-number {in | out}
```

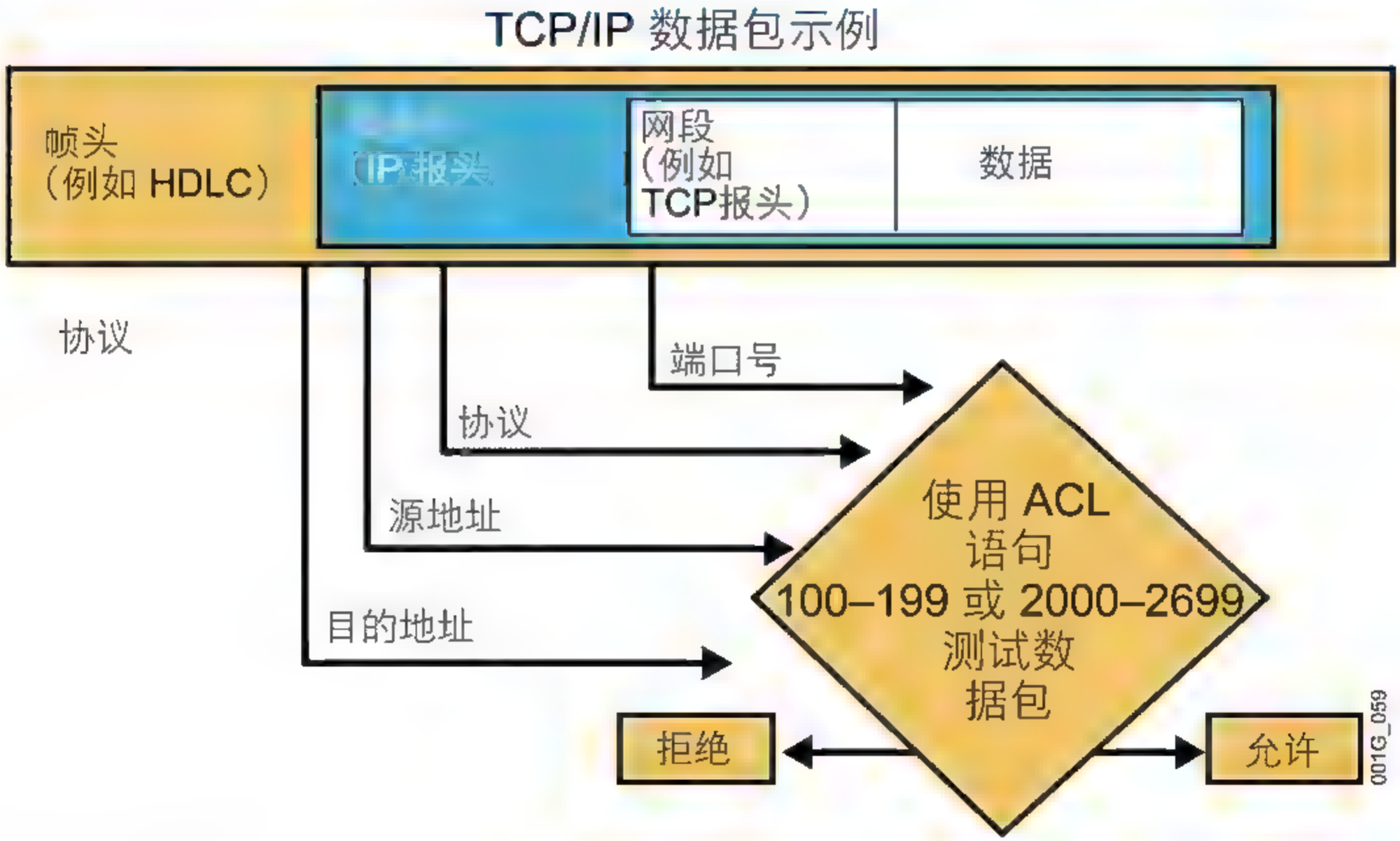
- 限制特定 vty 与 ACL 地址之间的入站或出站连接

示例：

```
access-list 12 permit 192.168.1.0 0.0.0.255
(隐式拒绝所有)
!
line vty 0 4
access-class 12 in
```

- 仅允许网络 192.168.1.0 0.0.0.255 中的主机连接到路由器的 vty 线路

用扩展编号 IPv4 ACL 测试数据包



扩展编号 IPv4 ACL 的配置

RouterX(config)#

```
access-list access-list-number {permit | deny}
protocol source source-wildcard [operator port]
destination destination-wildcard [operator port]
[established] [log]
```

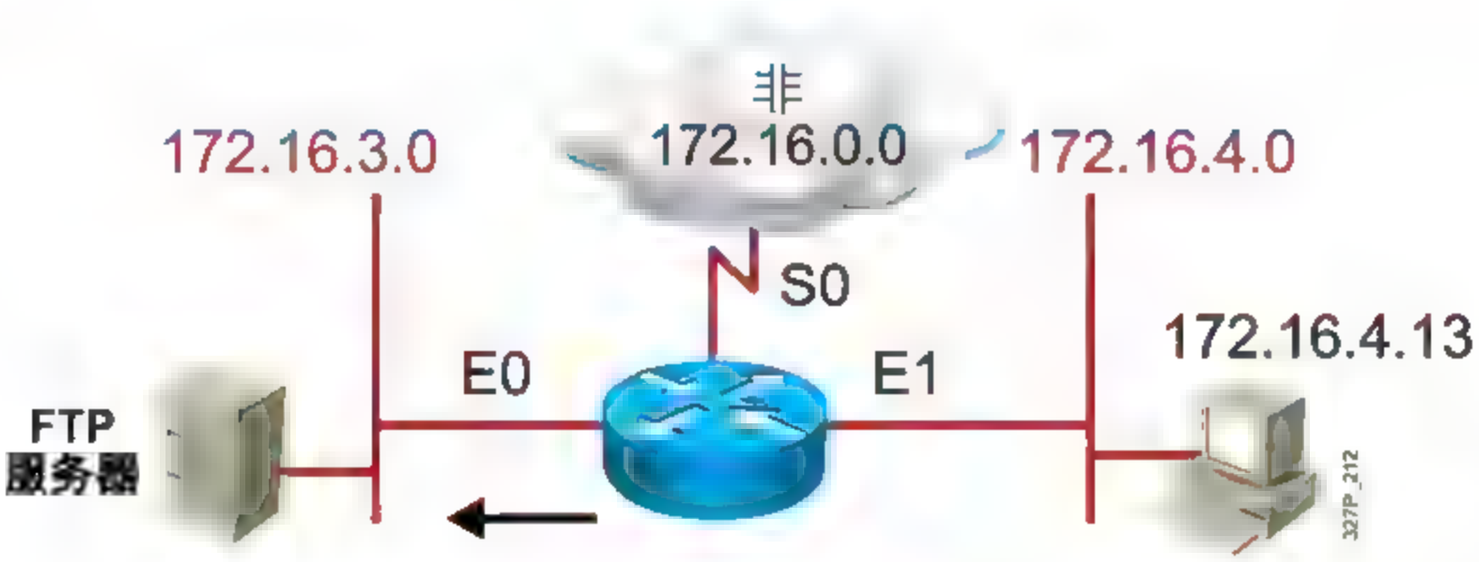
- 设置此列表条目的参数

RouterX(config-if)#

```
ip access-group access-list-number  {in | out}
```

- 激活接口上的扩展列表

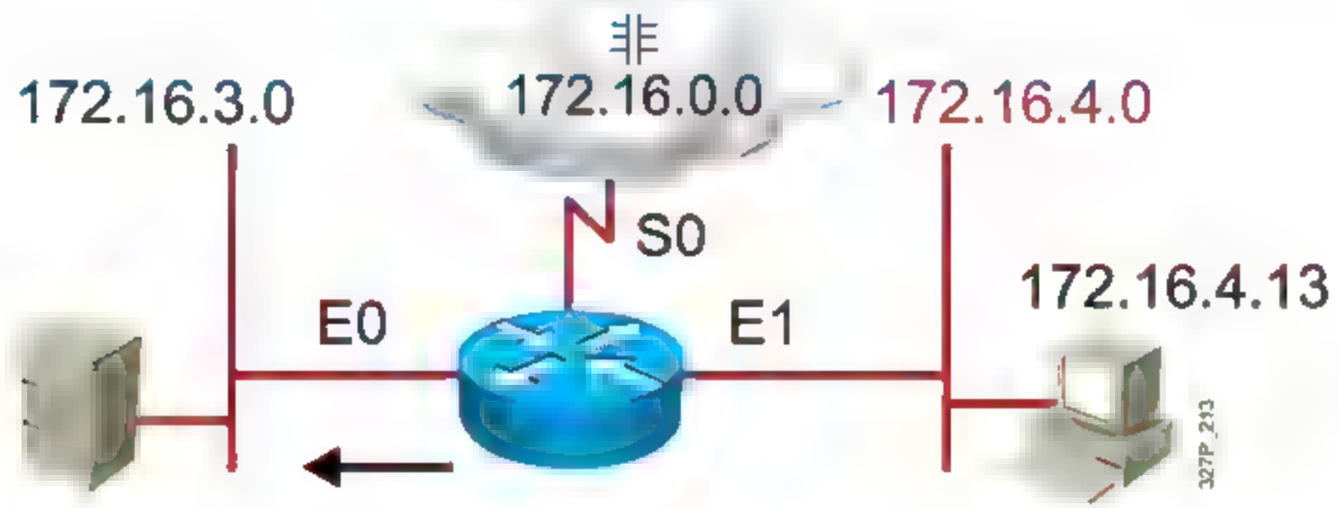
扩展编号 IPv4 ACL 示例 1




```
RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
RouterX(config)# access-list 101 permit ip any any
(隐式拒绝所有)
(access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 101 out
```

- 拒绝从子网 172.16.4.0 到子网 172.16.3.0 经 E0 流出的 FTP 流量
- 允许所有其它流量

扩展编号 IPv4 ACL 示例 2




```
RouterX(config)# access-list 101 deny tcp 172.16.4.0  0.0.0.255  any eq 23
RouterX(config)# access-list 101 permit ip any any
(隐式拒绝所有)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 101 out
```

- 仅拒绝来自子网 172.16.4.0 经 E0 流出的 Telnet 流量
- 允许所有其它流量

命名 IP ACL 的配置

RouterX(config)#

```
ip access-list {standard | extended} name
```

- 字母数字命名的字符串必须是唯一的

RouterX(config {std- | ext-}nacl)#

```
[sequence-number] {permit | deny} {ip access list test conditions}
{permit | deny} {ip access list test conditions}
```

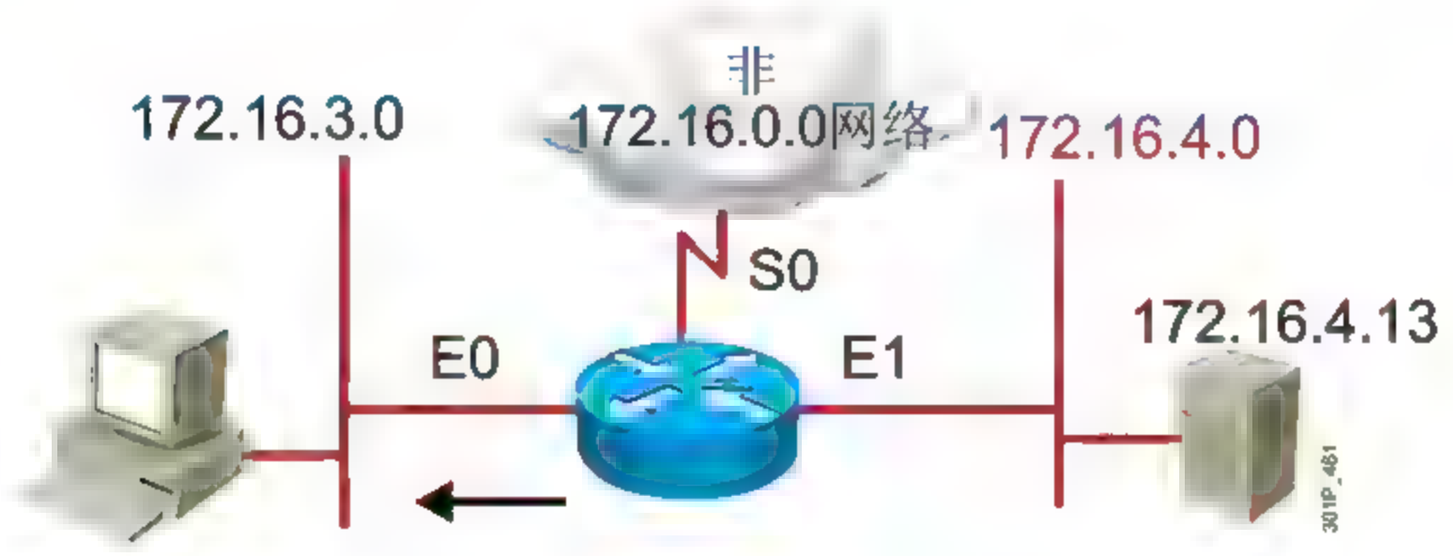
- 如果未配置，则从 10 开始自动生成序列号，
  并以 10 为增量递增
- **no***序列号*命令可从命名 ACL 中删除指定测试

RouterX(config-if)#

```
ip access-group name {in | out}
```

- 激活接口上的命名 IP ACL

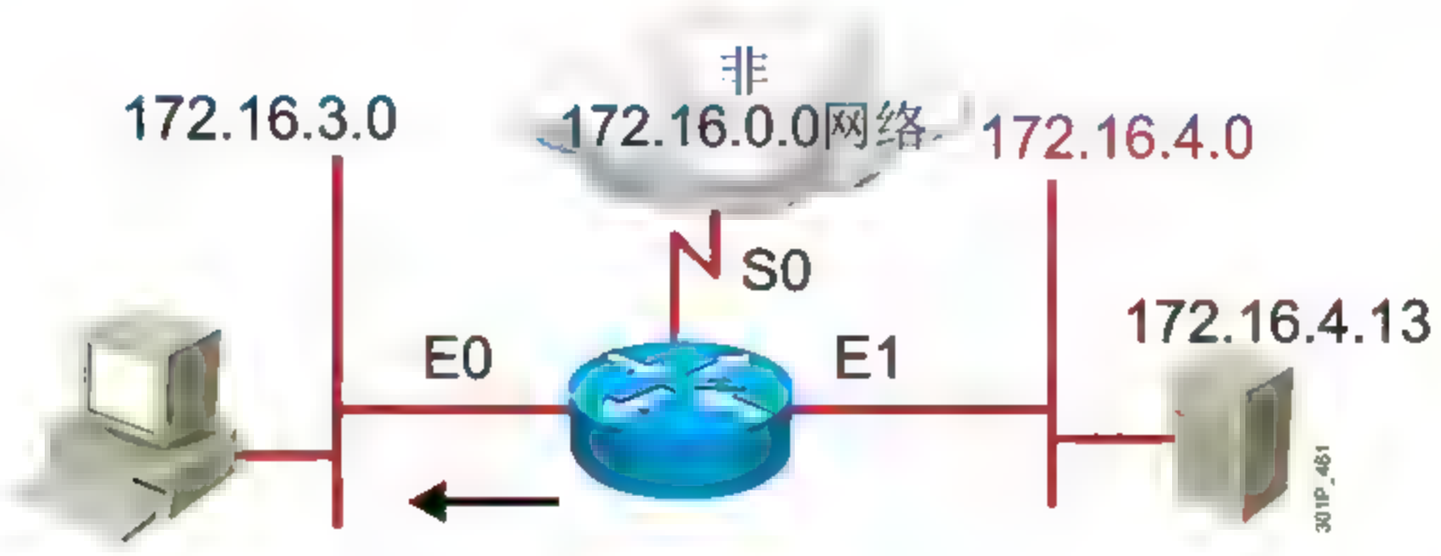
标准命名 IPv4 ACL 示例




```
RouterX(config)#ip access-list standard troublemaker
RouterX(config-std-nacl)#deny host 172.16.4.13
RouterX(config-std-nacl)#permit 172.16.4.0 0.0.0.255
RouterX(config-std-nacl)#interface e0
RouterX(config-if)#ip access-group troublemaker out
```

拒绝特定的主机

扩展命名 IPv4 ACL 示例




```
RouterX(config)#ip access-list extended badgroup
RouterX(config-ext-nacl)#deny tcp 172.16.4.0 0.0.0.255 any eq 23
RouterX(config-ext-nacl)#permit ip any any
RouterX(config-ext-nacl)#interface e0
RouterX(config-if)#ip access-group badgroup out
```

拒绝来自特定子网的 Telnet 流量

注释 ACL 语句

```
RouterX(config)#
ip access-list {standard|extended} name
```

- 创建命名 ACL

```
RouterX(config {std- | ext-}nacl)#
remark remark
```

- 创建命名 ACL 注释

或

```
RouterX(config)#
access-list access-list-number remark remark
```

- 创建被编号的 ACL 注释

监控 ACL 语句

```
RouterX# show access-lists {access-list number|name}
```

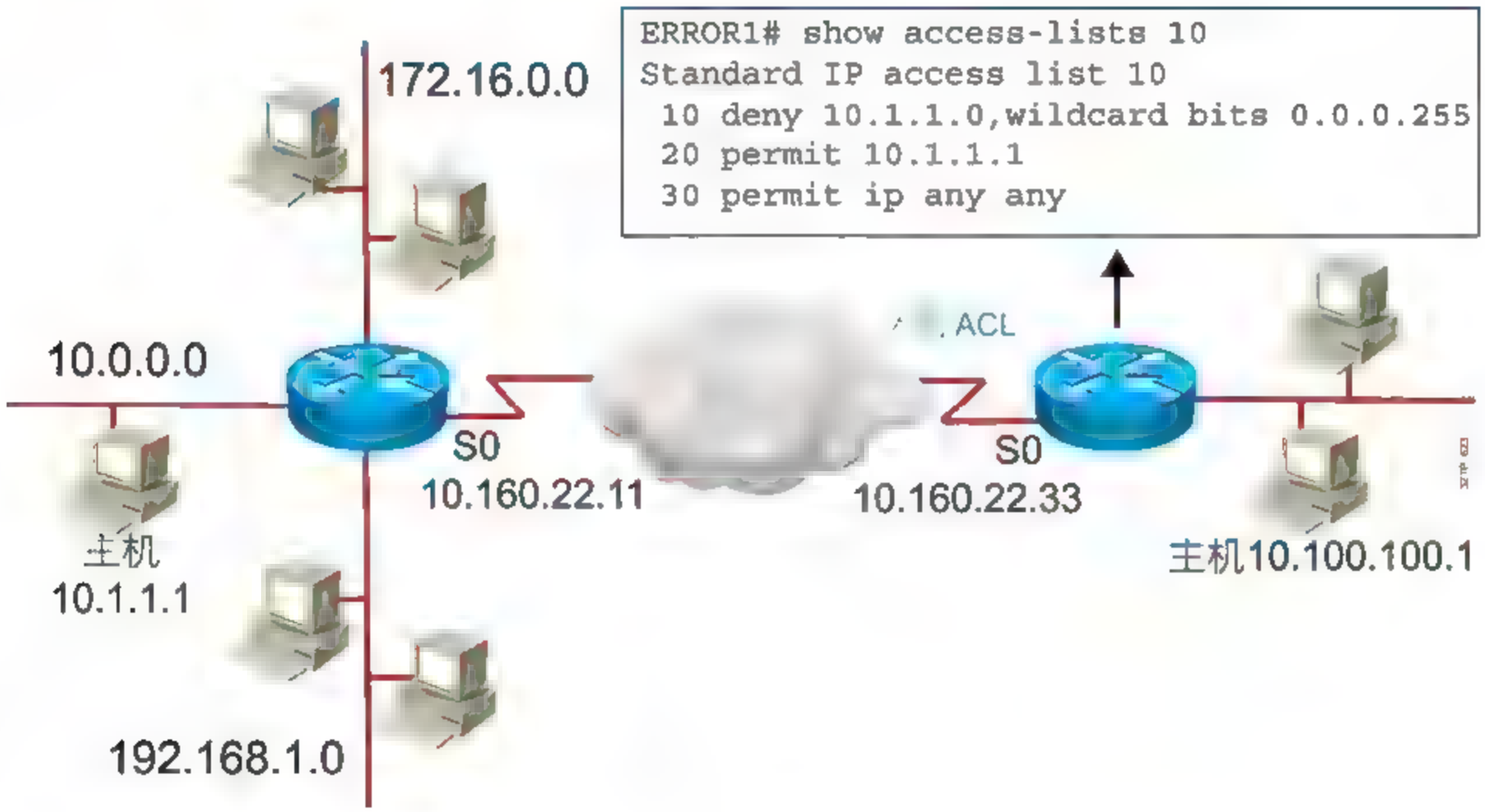
```
RouterX# show access-lists
Standard IP access list SALES
10 deny   10.1.1.0, wildcard bits 0.0.0.255
20 permit 10.3.3.1
30 permit 10.4.4.1
40 permit 10.5.5.1
Extended IP access list ENG
10 permit tcp host 10.22.22.1 any eq telnet (25 matches)
20 permit tcp host 10.33.33.1 any eq ftp
30 permit tcp host 10.44.44.1 any eq ftp-data
```

显示所有访问列表

检验 ACL

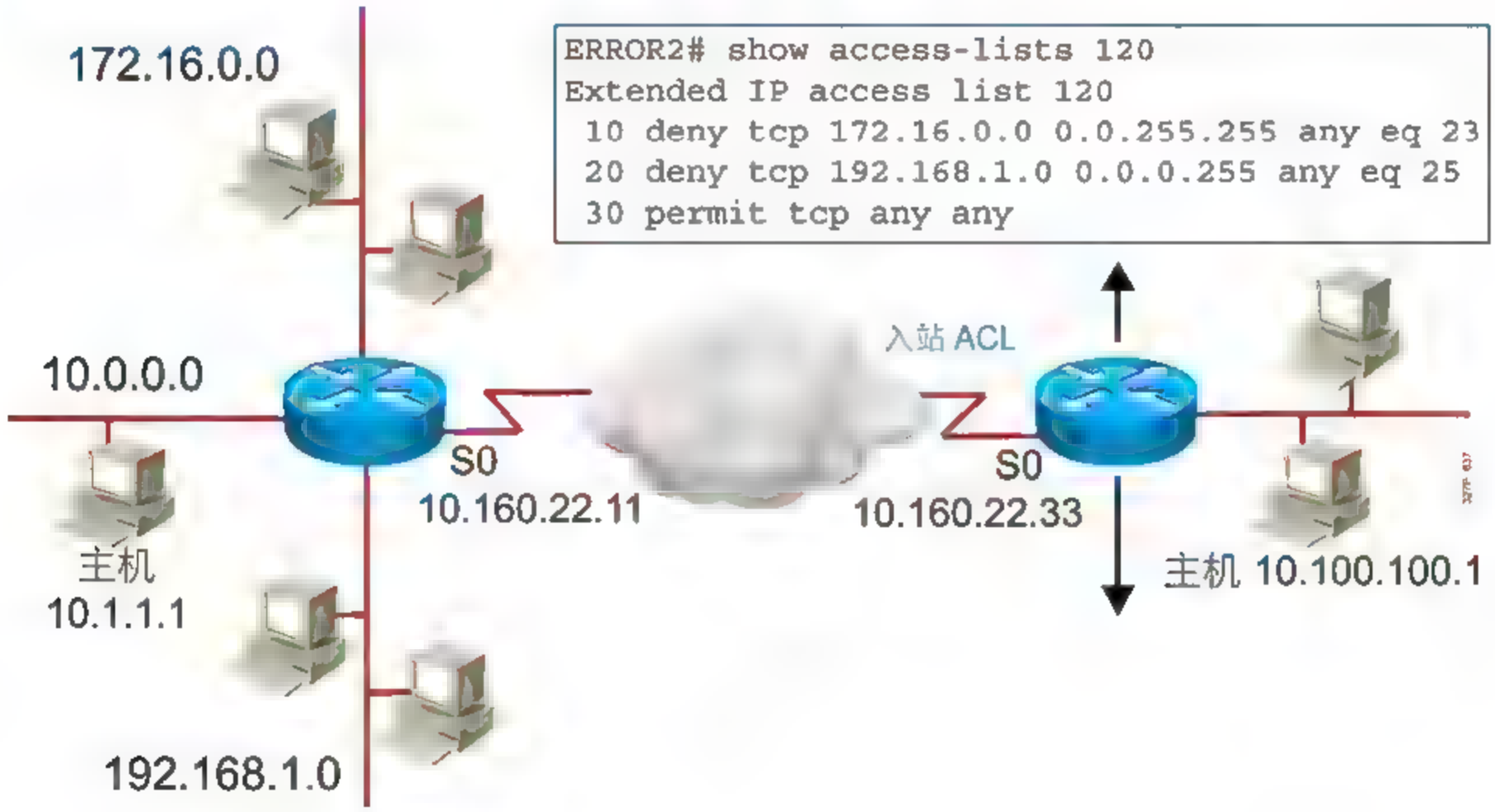
```
RouterX# show ip interfaces e0
Ethernet0 is up, line protocol is up
  Internet address is 10.1.1.11/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 1
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  <省略部分文本>
```

排除 ACL 的常见错误



错误 1：主机 10.1.1.1 与 10.100.100.1 没有连接。

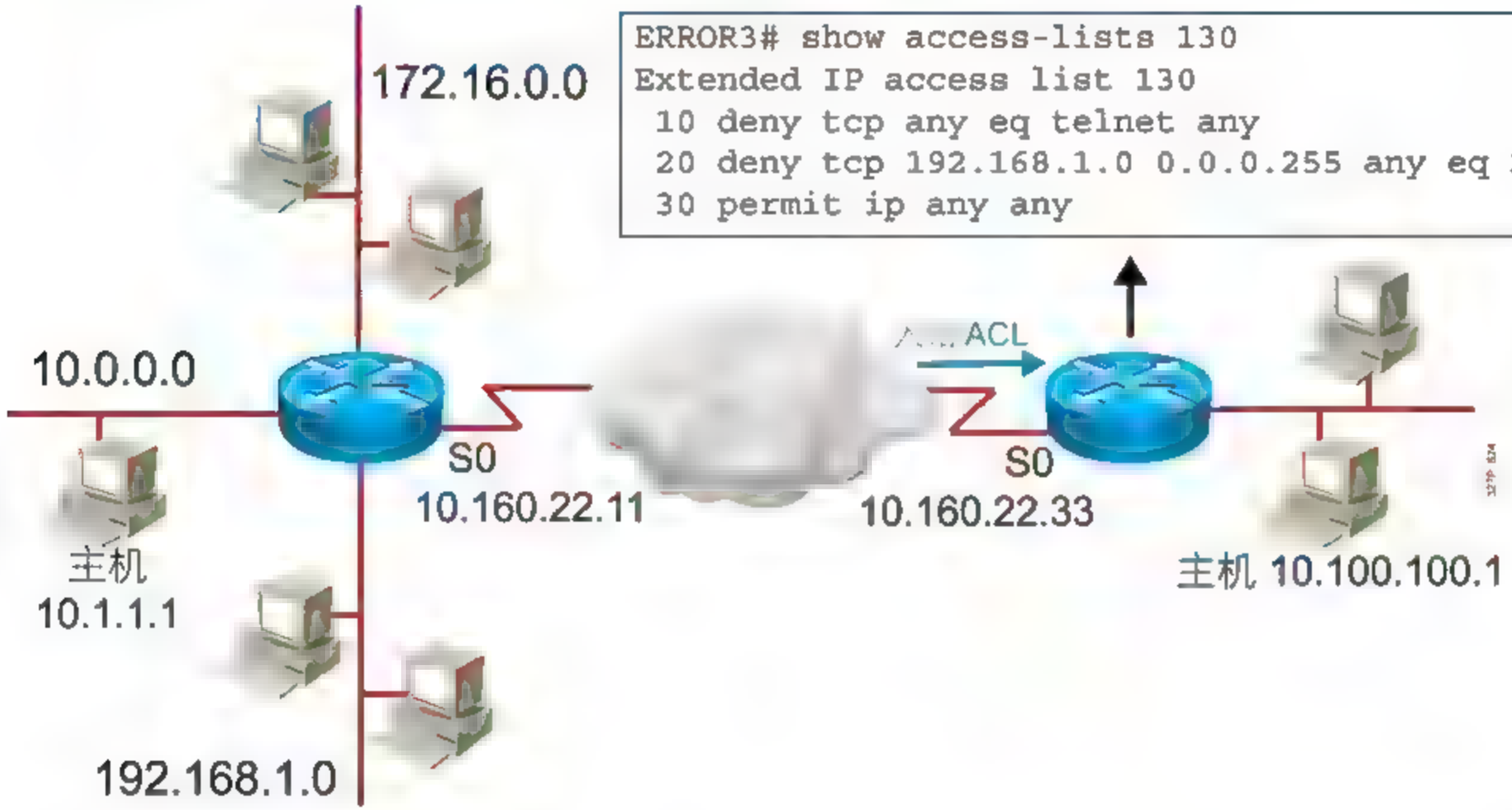
排除 ACL 的常见错误（续）




```
ERROR2# show access-lists 120
Extended IP access list 120
 10 deny tcp 172.16.0.0 0.0.255.255 any eq 23
 20 deny tcp 192.168.1.0 0.0.0.255 any eq 25
 30 permit tcp any any
```

错误 2：192.168.1.0 网络无法用 TFTP 连接 10.100.100.1。

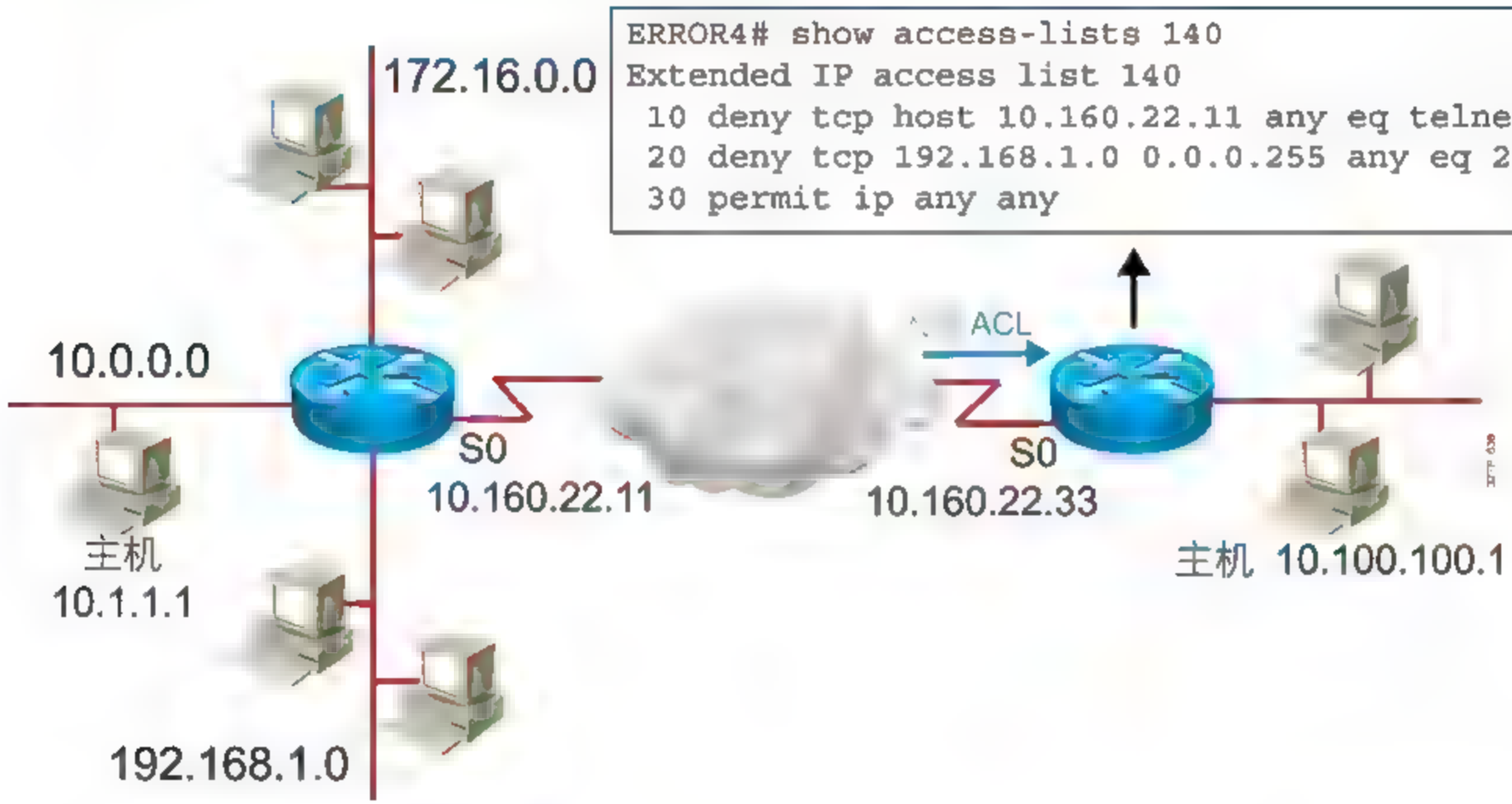
排除 ACL 的常见错误（续）




```
ERROR3# show access-lists 130
Extended IP access list 130
 10 deny tcp any eq telnet any
 20 deny tcp 192.168.1.0 0.0.0.255 any eq 25
 30 permit ip any any
```

错误 3：172.16.0.0 网络可使用 Telnet 连接 10.100.100.1，但是不允许进行此项连接。

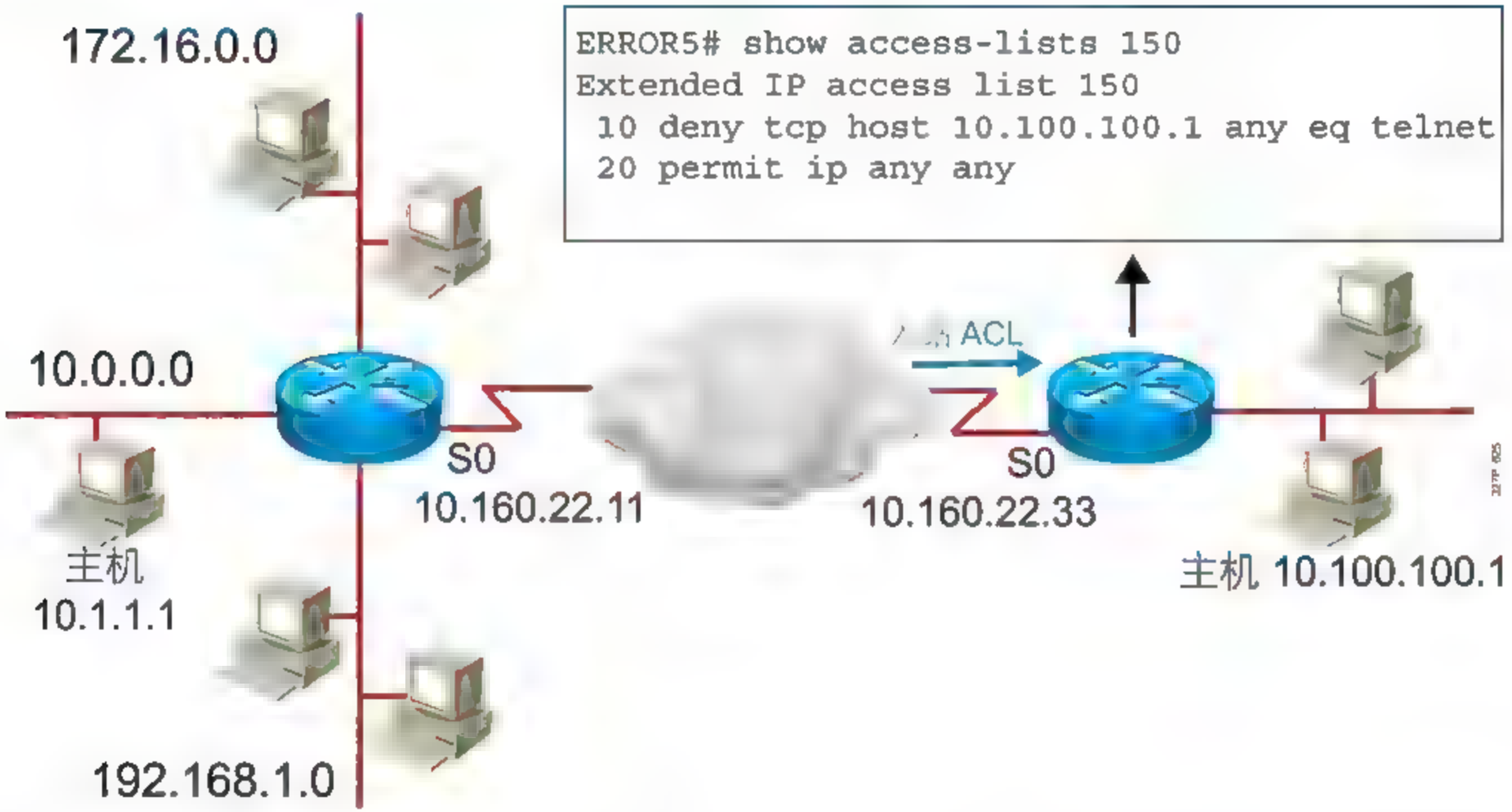
排除 ACL 的常见错误（续）



错误 4：主机 10.1.1.1 可使用 Telnet 连接 10.100.100.1，但是不允许进行此项连接。

© 2008 Cisco Systems, Inc. 保留一切权利。

排除 ACL 的常见错误（续）

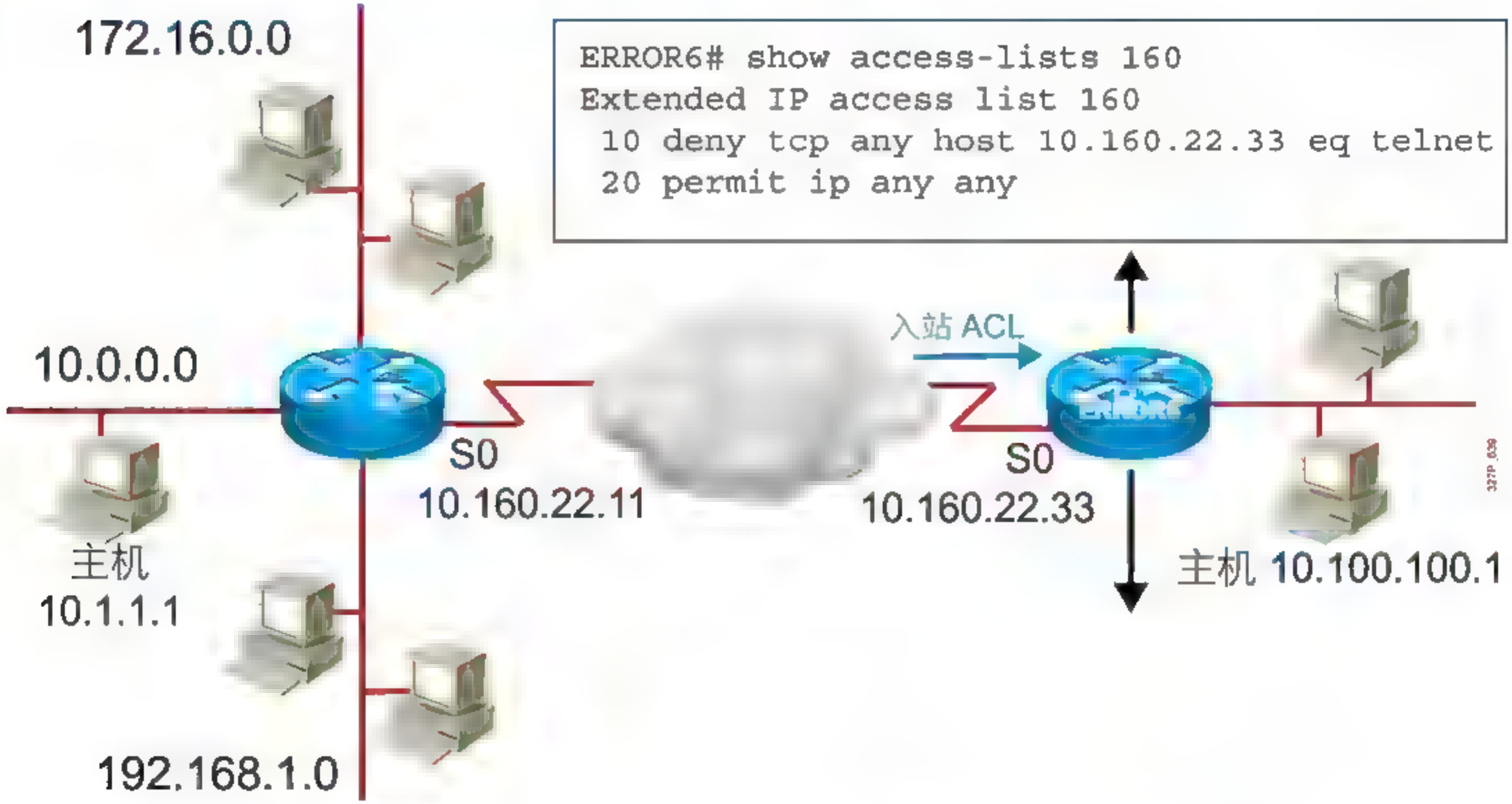



```
ERROR5# show access-lists 150
Extended IP access list 150
 10 deny tcp host 10.100.100.1 any eq telnet
 20 permit ip any any
```

错误 5：主机 10.100.100.1 可使用 Telnet 连接 10.1.1.1，但是不允许进行此项连接。

© 2008 Cisco Systems, Inc. 保留所有权利。

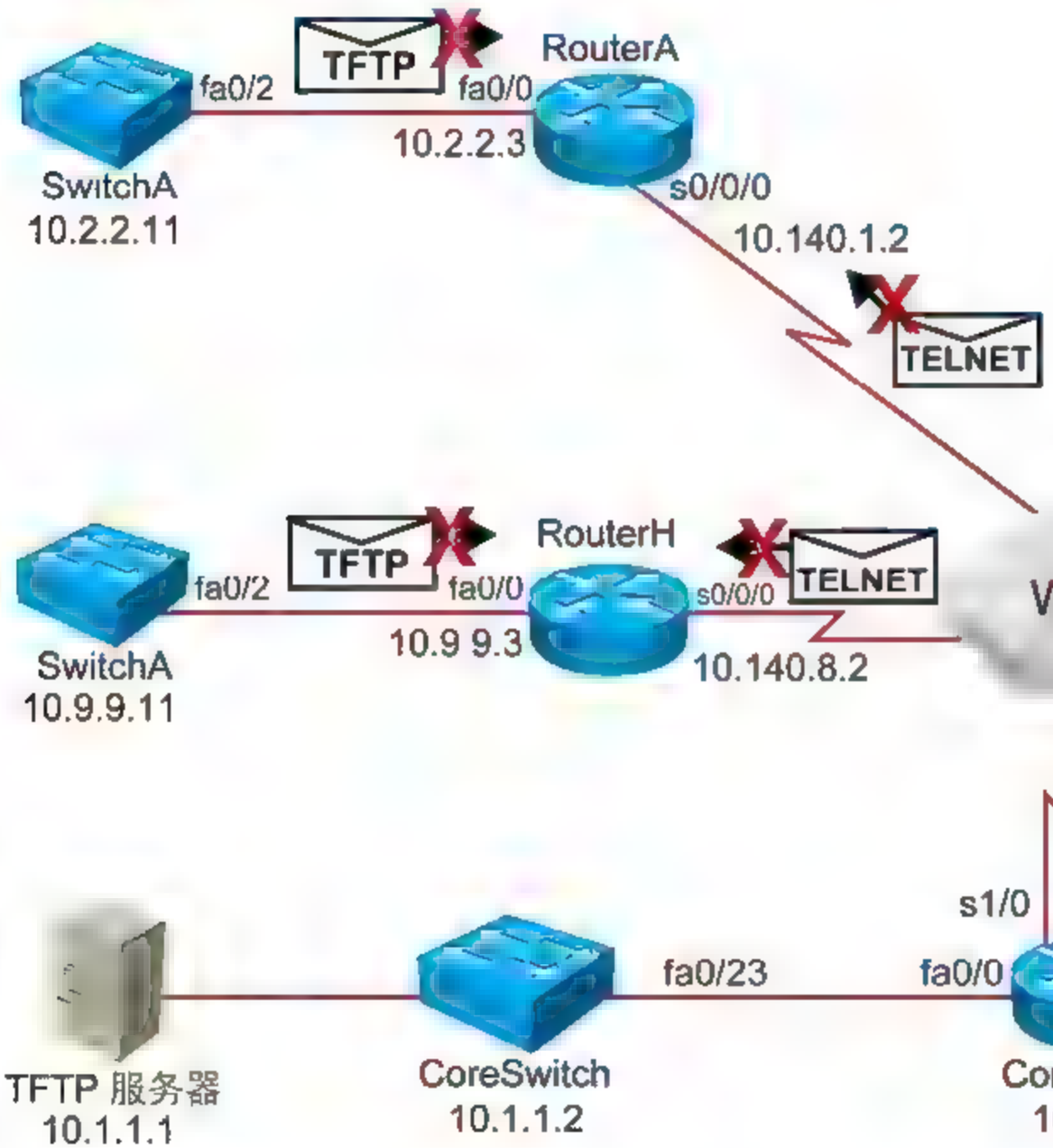
排除 ACL 的常见错误（续）



错误 6：主机 10.1.1.1 可使用 Telnet 连接路由器 B，但是不允许进行此项连接。

Systems Inc. 保留所有权利。

可视目标 6-1：ACL 实施与故障排除



工作组	路由器 s0/0/0	路由器 fa0/0	交换机
A	10.140.1.2	10.2.2.3	10.2.2.11
B	10.140.2.2	10.3.3.3	10.3.3.11
C	10.140.3.2	10.4.4.3	10.4.4.11
D	10.140.4.2	10.5.5.3	10.5.5.11
E	10.140.5.2	10.6.6.3	10.6.6.11
F	10.140.6.2	10.7.7.3	10.7.7.11
G	10.140.7.2	10.8.8.3	10.8.8.11
H	10.140.8.2	10.9.9.3	10.9.9.11

总结

- 标准 IPv4 ACL 允许根据源 IP 地址进行过滤。
- 扩展 ACL 允许根据源 IP 地址、目的 IP 地址、协议和端口号进行过滤。
- 指定 ACL 允许从一条 ACL 中删除单条语句。
- 可使用 **show access-lists** 和 **show ip interface** 命令排除 ACL 配置的常见错误。

CISCO

单元总结

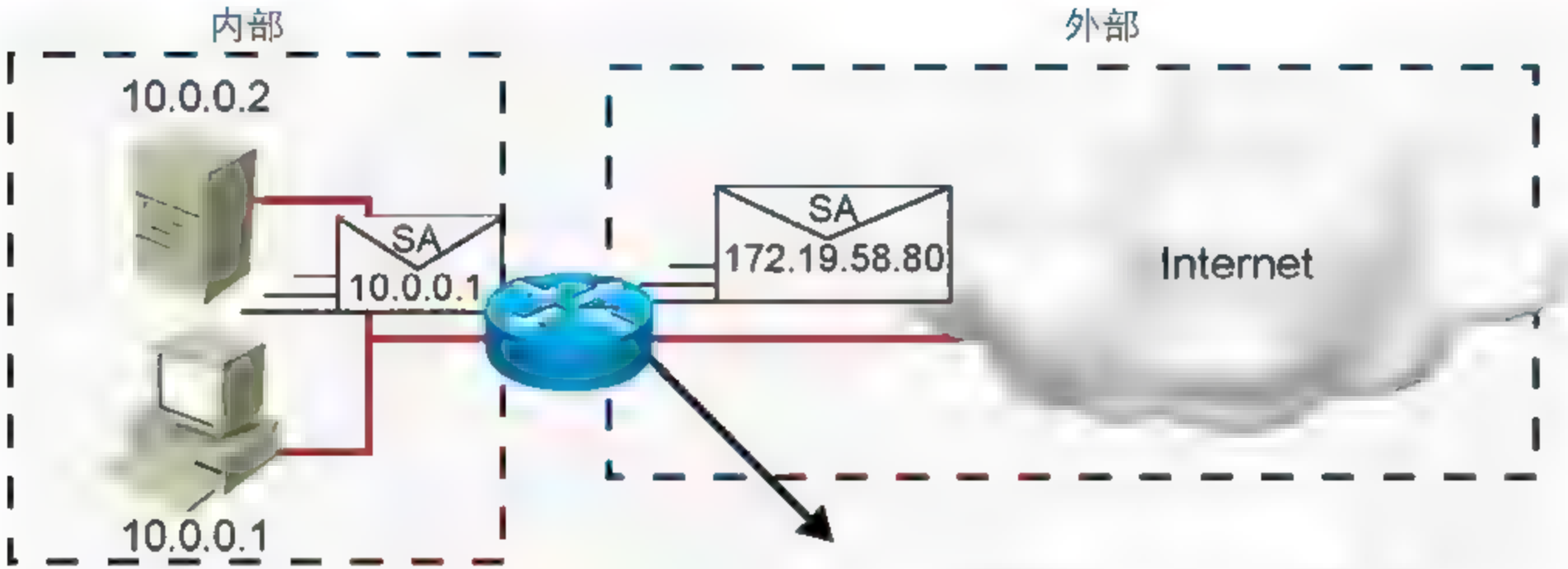
- ACL 可用于为特定处理过滤 IP 数据包或标识流量。
- ACL 执行自上而下的处理过程，可针对入站流量或出站流量进行配置。
- 在通配符位掩码中，0 表示匹配对应地址位，1 表示忽略对应地址位。
- 标准 IPv4 ACL 允许根据源地址进行过滤。
- 扩展 IPv4 ACL 允许根据源地址和目的地址以及协议和端口号进行过滤。
- IP 访问列表条目序列编号允许从 ACL 中删除单条语句以便在 ACL 的任意位置添加语句。
- **show access-lists** 和 **show ip interface** 命令用于排除 ACL 常见的配置错误。

CISCO

使用 NAT 和 PAT 扩展网络

地址空间管理

网络地址转换



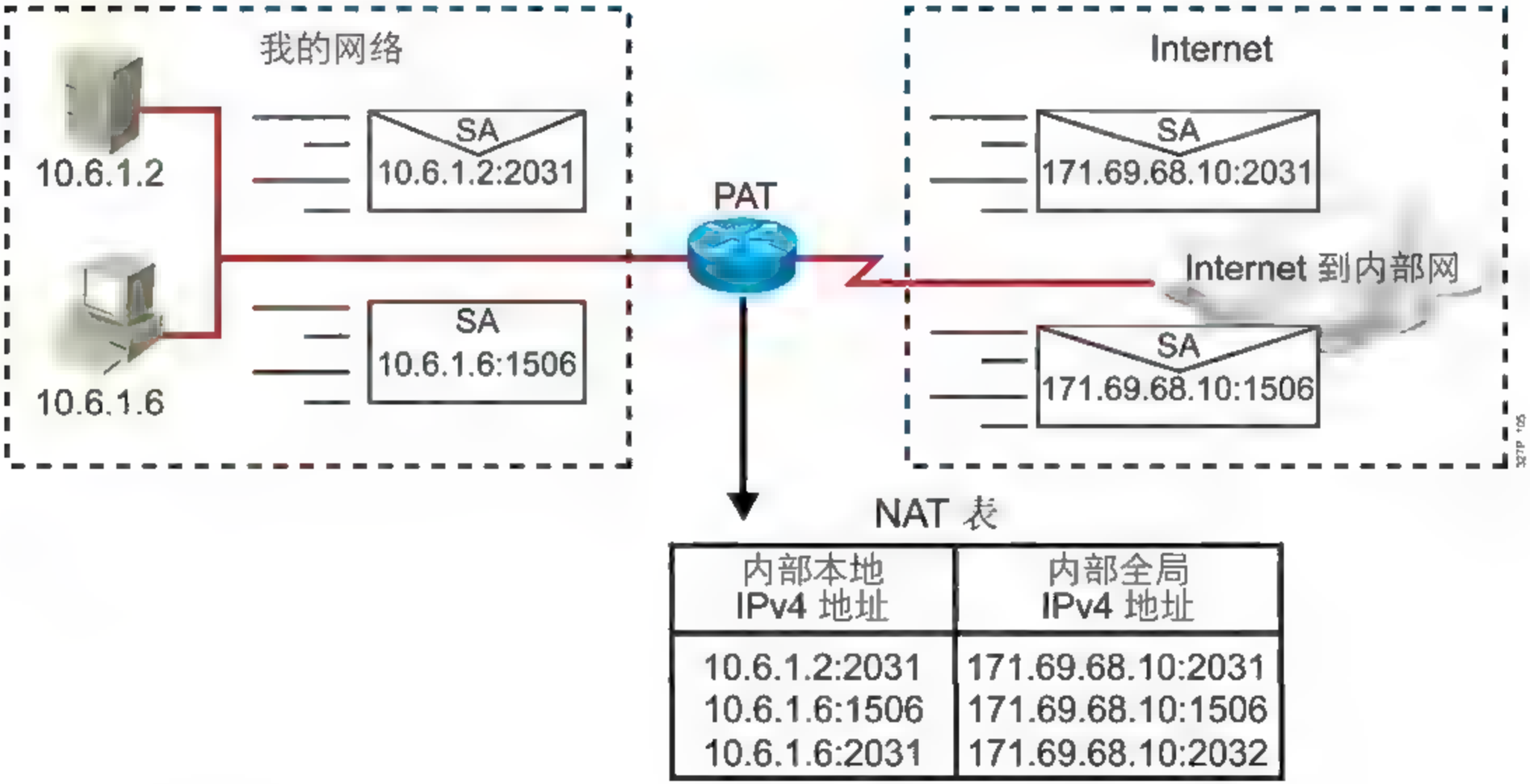
内部本地 IPv4 地址	内部全局 IPv4 地址
10.0.0.1 10.0.0.2	172.19.58.80 172.19.58.81

327P_205

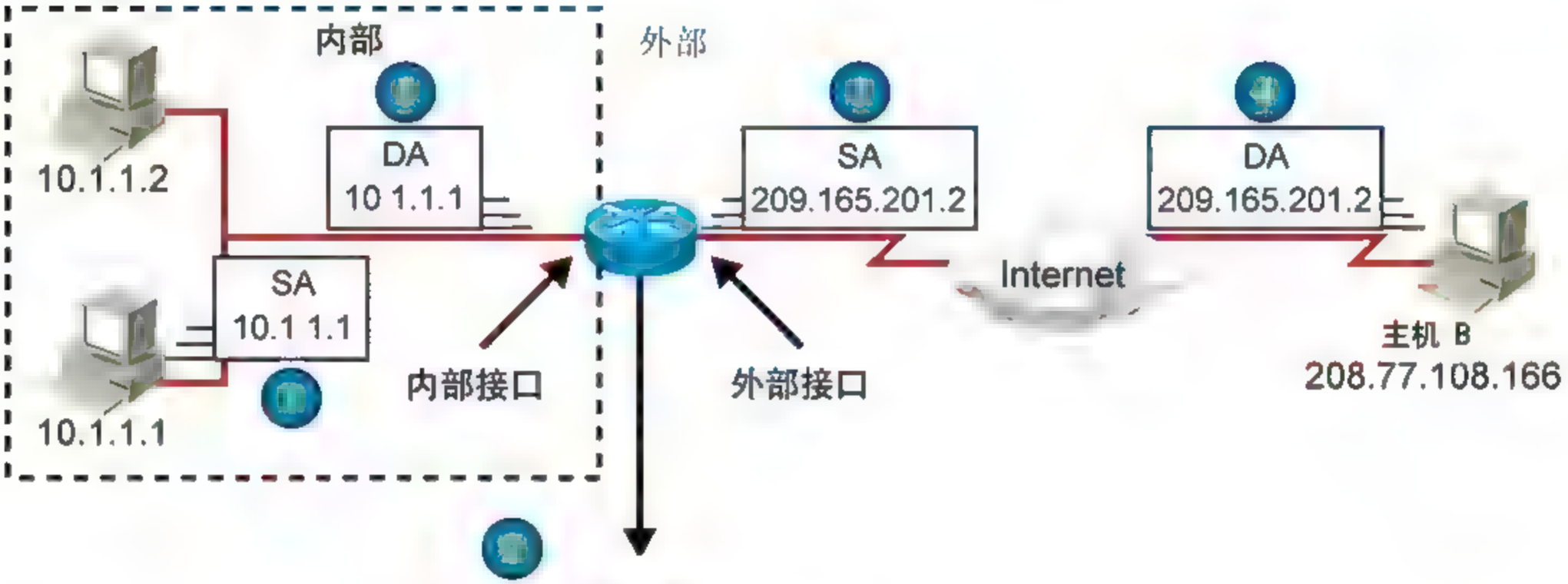
- IP 地址是本地地址或全局地址。
- 本地 IPv4 地址在网络内部可见。
- 全局 IPv4 地址在网络外部可见。

保留所有权利。

端口地址转换


我的网络
10.6.1.2
SA
10.6.1.2:2031
10.6.1.6
SA
10.6.1.6:1506
PAT
Internet
SA
171.69.68.10:2031
Internet 到内部网
SA
171.69.68.10:1506
NAT 表
内部本地 IPv4 地址
内部全局 IPv4 地址
10.6.1.2:2031
171.69.68.10:2031
10.6.1.6:1506
171.69.68.10:1506
10.6.1.6:2031
171.69.68.10:2032

转换内部源地址



NAT 表

内部本地 IPv4 地址	内部全局 IPv4 地址
10.1.1.2	209.165.201.3
10.1.1.1	209.165.201.2

配置和检验静态转换

```
RouterX(config)# ip nat inside source static local-ip global-ip
```

- 建立内部本地地址与内部全局地址间的静态转换

```
RouterX(config-if)# ip nat inside
```

- 将该接口标记为连接内部网络的接口

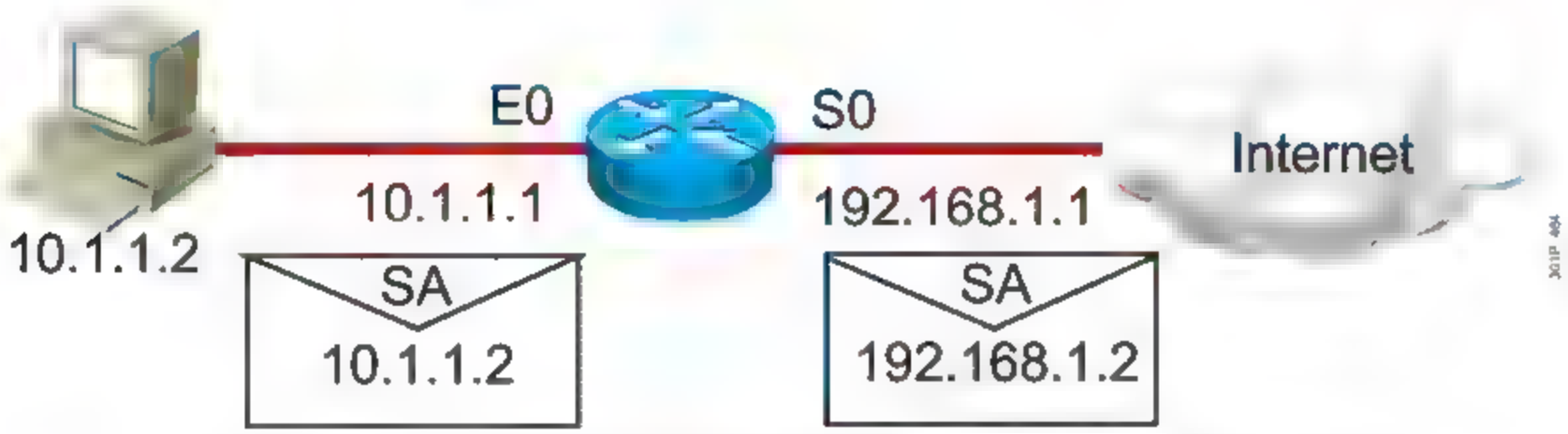
```
RouterX(config-if)# ip nat outside
```

- 将该接口标记为连接外部网络的接口

```
RouterX# show ip nat translations
```

- 显示活动的转换

启用静态 NAT 地址映射示例




```
interface s0
ip address 192.168.1.1 255.255.255.0
ip nat outside
!
interface e0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
ip nat inside source static 10.1.1.2 192.168.1.2
```

```
RouterX# show ip nat translations
      Pro Inside global   Inside local   Outside local   Outside global
      --- 192.168.1.2       10.1.1.2          ---              ---
```

配置和检验动态转换

```
RouterX(config)# ip nat pool name start-ip end-ip
{netmask netmask | prefix-length prefix-length}
```

- 定义可根据需要进行分配的全局地址池

```
RouterX(config)# access-list access-list-number permit
source [source-wildcard]
```

- 定义允许那些要被转换的内部本地地址的标准 IP ACL

```
RouterX(config)# ip nat inside source list
access-list-number pool name
```

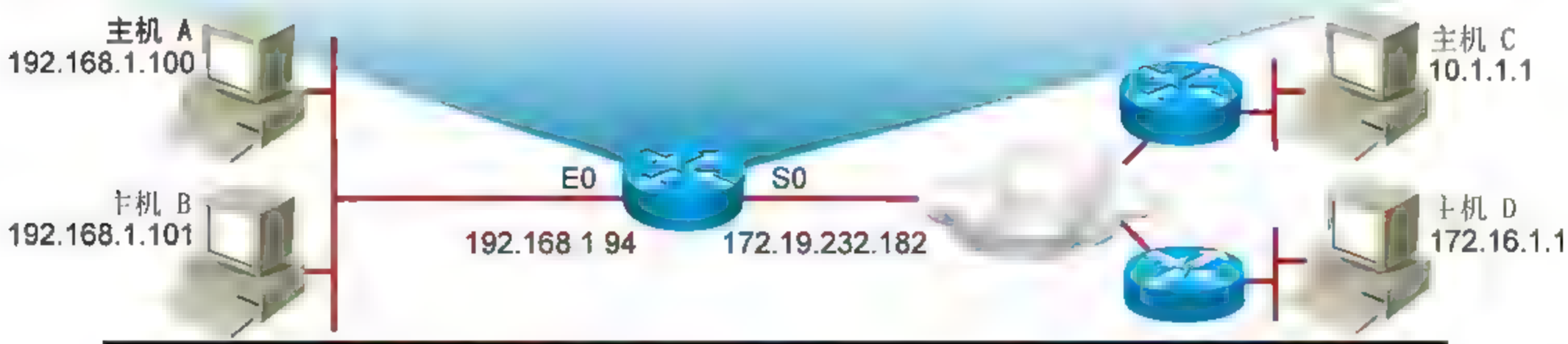
- 建立动态源转换，指定上一步定义的 ACL

```
RouterX# show ip nat translations
```

- 显示活动的转换

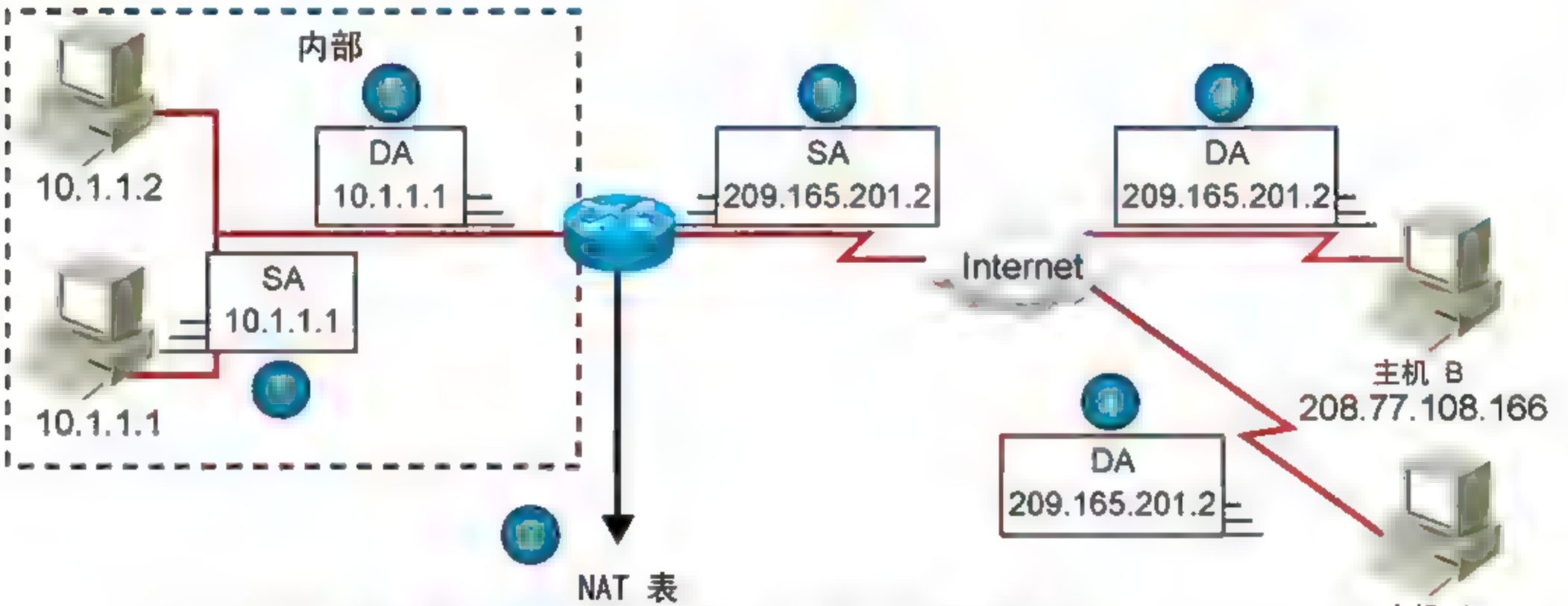
动态地址转换示例

```
ip nat pool net-208 172.19.233.209 172.19.233.222 netmask 255.255.255.240
ip nat inside source list 1 pool net-208
!
interface serial 0
 ip address 172.19.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 0
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```




```
RouterX# show ip nat translations
    Pro Inside global     Inside local      Outside local     Outside global
    --- 172.19.233.209    192.168.1.100     ---               ---
    --- 172.19.233.210    192.168.1.101     ---               ---
```

过载内部全局地址



NAT 表

协议	内部本地 ipv4 地址：端口	内部全局 ipv4 地址：端口	外部全局 ipv4 地址：端口
TCP	10 1 1 2:1723	209 165 201 2 1723	209 165 202 158 23
TCP	10 1.1.1.1024	209.165.201.2.1024	208.77.108.166.23

327P_208

配置过载

```
RouterX(config)# access-list access-list-number permit
source source-wildcard
```

- 定义允许那些要被转换的内部本地地址的标准 IP ACL

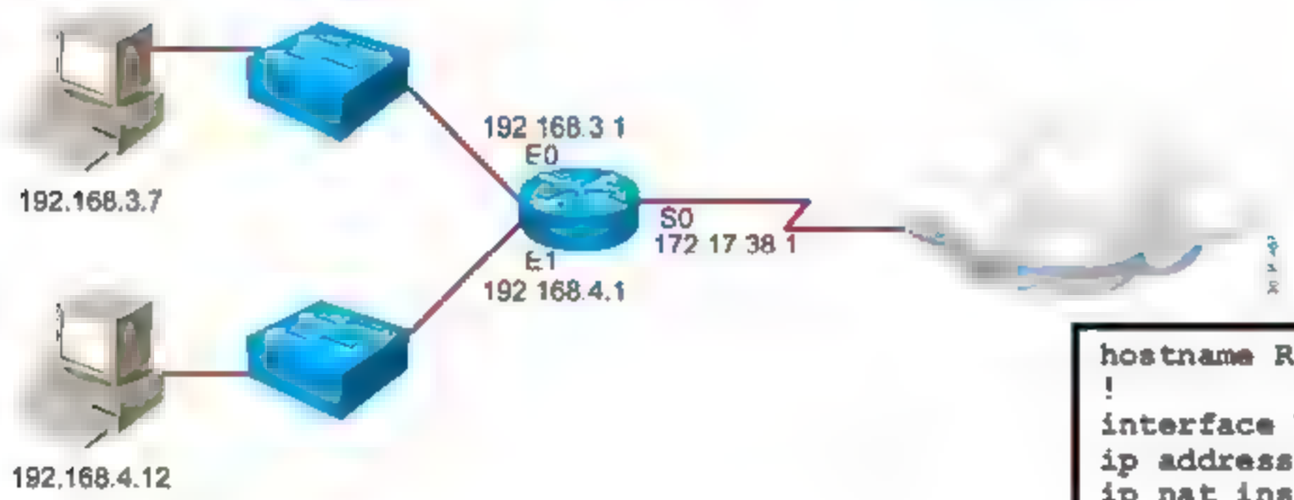
```
RouterX(config)# ip nat inside source list
access-list-number interface interface overload
```

- 建立动态源转换，指定上一步定义的 ACL

```
RouterX# show ip nat translations
```

- 显示活动的转换

过载内部全局地址示例




```
hostname RouterX
!
interface Ethernet0
ip address 192.168.3.1 255.255.255.0
ip nat inside
!
interface Ethernet1
ip address 192.168.4.1 255.255.255.0
ip nat inside
!
interface Serial0
description To ISP
ip address 172.17.38.1 255.255.255.0
ip nat outside
!
ip nat inside source list 1 interface Serial0 overload
!
ip route 0.0.0.0 0.0.0.0 Serial0
!
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.0.255
!
```

```
RouterX# show ip nat translations
     Pro Inside global      Inside local       Outside local      Outside global
     TCP 172.17.38.1:1050   192.168.3.7:1050    10.1.1.1:23        10 1.1.1:23
TCP 172.17.38.1:1776   192.168.4.12:1776   10.2.2.2:25        10.2.2.2:25
```

清除 NAT 转换表

```
RouterX# clear ip nat translation *
```

- 清除所有动态地址转换条目

```
RouterX# clear ip nat translation inside global-ip
local-ip [outside local-ip global-ip]
```

- 清除包含内部转换或同时包含内部转换与外部转换的简单动态转换条目

```
RouterX# clear ip nat translation outside
local-ip global-ip
```

- 清除包含外部转换的简单动态转换条目

```
RouterX# clear ip nat translation protocol inside global-ip
global-port local-ip local-port [outside local-ip
local-port global-ip global-port]
```

- 清除扩展动态转换条目（PAT 条目）

未执行转换：
转换表中没有包含转换

检验：

- 不存在拒绝数据包进入 NAT 路由器的入站 ACL
- NAT 命令所引用的 ACL 是否允许所有必需的网络
- NAT 池中是否有足够的地址
- 路由器接口是否被正确定义为 NAT 内部接口或 NAT 外部接口

© 2008 Cisco Systems, Inc. 保留所有权利

用 show 和 debug 命令显示信息

```
RouterX# debug ip nat

NAT:s=192.168.1.95->172.31.233.209, d=172.31.2.132 [6825]
NAT:s=172.31.2.132, d=172.31.233.209->192.168.1.95 [21852]
NAT:s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6826]
NAT*:s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23311]
NAT*:s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6827]
NAT*:s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6828]
NAT*:s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23312]
NAT*:s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23313]
```

```
RouterX# show ip nat statistics
      Total active translations:1 (1 static, 0 dynamic; 0 extended)
      Outside interfaces:
Ethernet0, Serial2
      Inside interfaces:
Ethernet1
      Hits:5  Misses: 0
      …
```

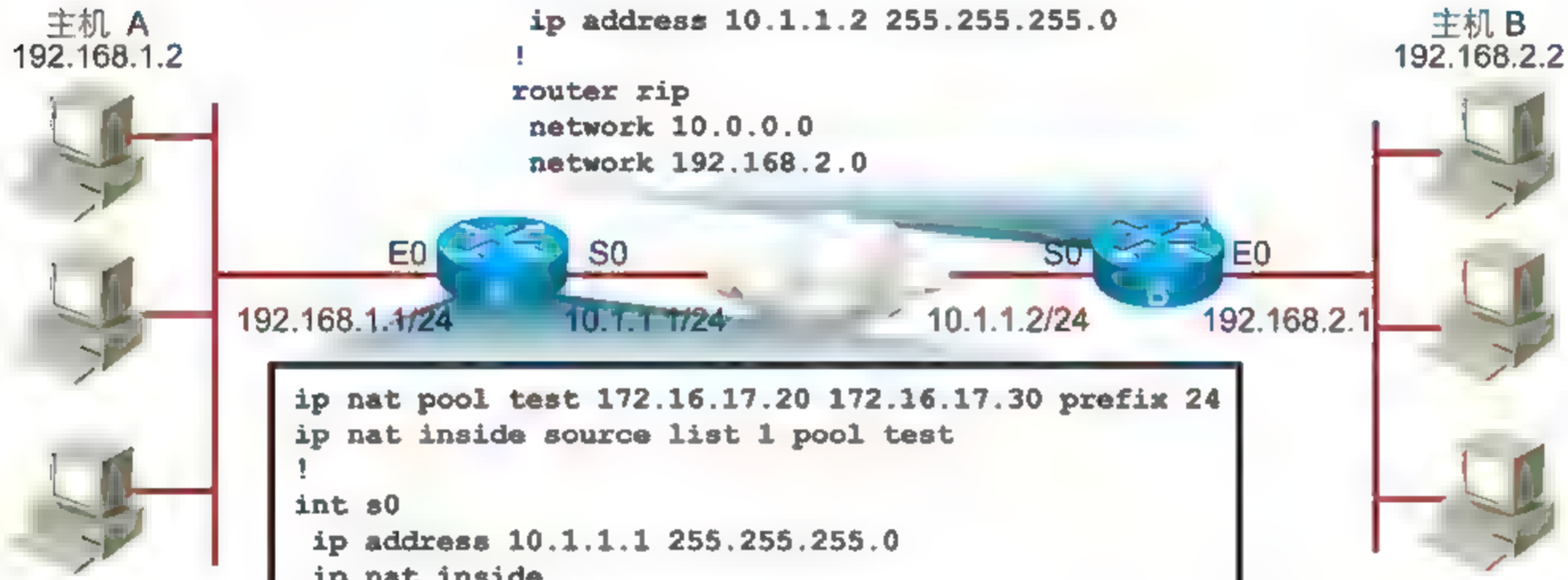
执行转换：已添加的未使用转换条目

检验：

- 应该完成什么样的 NAT 配置
- NAT 条目是否准确地存在于转换表中
- 实际上是否由监控 NAT 过程或统计信息引起转换
- 如果数据包从内部传向外部，那么 NAT 路由器的路由表中是否存在正确的路由
- 所有必需的路由器是否有回到转换后地址的返回路由

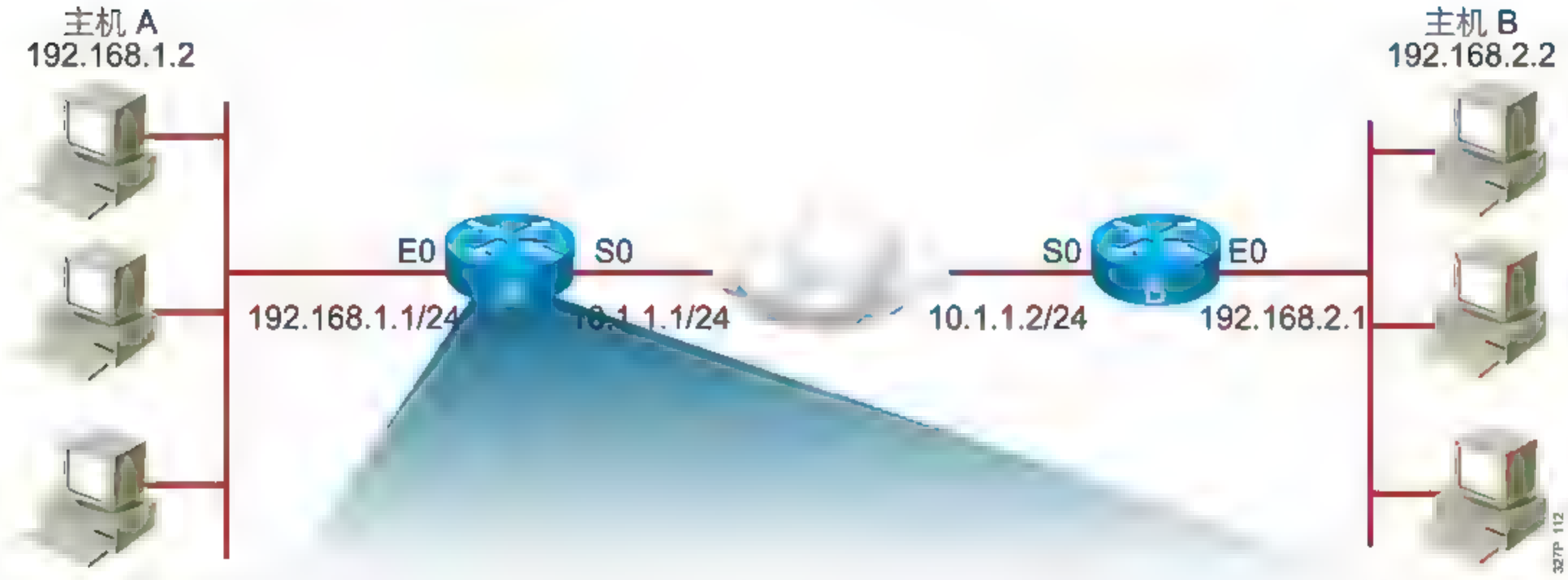
问题示例：无法 Ping 通远程主机

```
int eo
 ip address 192.168.2.1 255.255.255.0
!
int s0
 ip address 10.1.1.2 255.255.255.0
!
router rip
 network 10.0.0.0
 network 192.168.2.0
```




```
ip nat pool test 172.16.17.20 172.16.17.30 prefix 24
ip nat inside source list 1 pool test
!
int s0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
!

int e0
 ip address 192.168.1.1 255.255.255.0
 ip nat outside
!
router rip
 network 10.0.0.0
 network 192.168.1.0
!
access-list 1 permit 192.168.1.0 255.255.255.0
```

问题示例：无法 Ping 通远程主机（续）

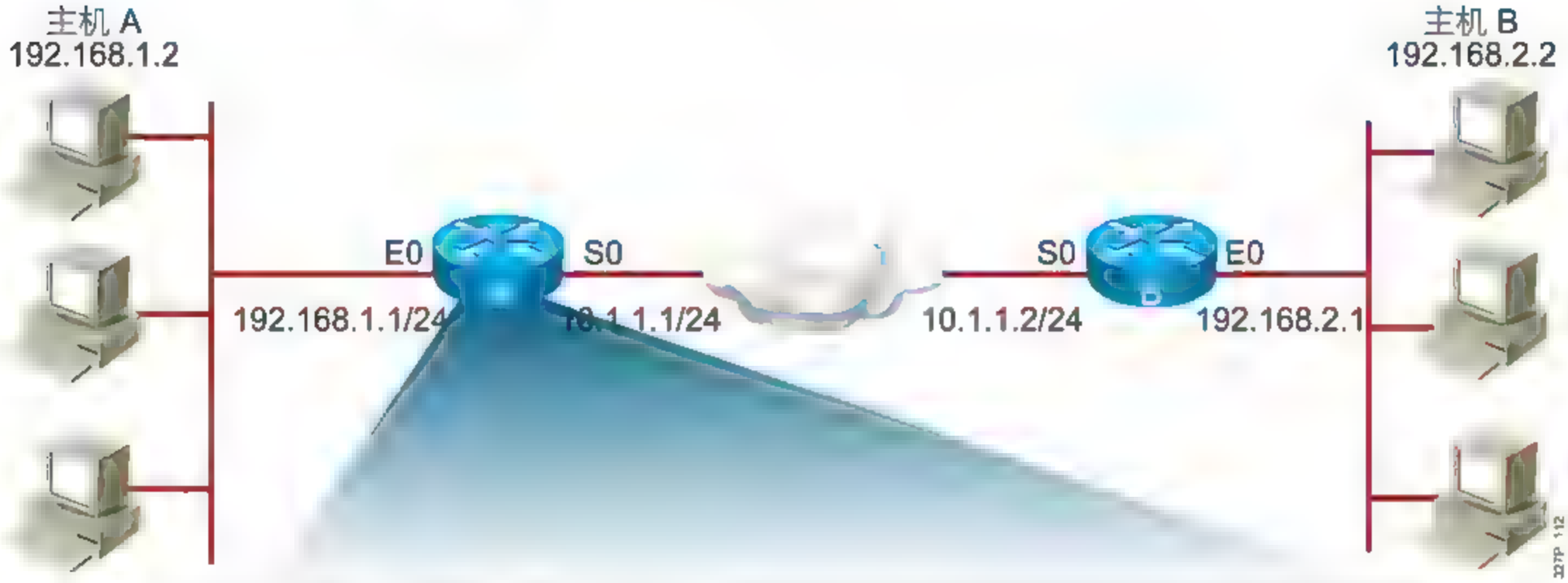



```
RouterA# show ip nat translations
      Pro Inside global     Inside local      Outside local     Outside global
      ---                                          ---               ---
      ---                                          ---               ---
```

转换表中无任何转换。

© 2008 Cisco Systems, Inc. 保留所有权利。

问题示例：无法 Ping 通远程主机（续）




```
RouterA# show ip nat statistics
      Total active translations:0 (0 static, 0 dynamic; 0 extended)
      Outside interfaces:
Ethernet0
      Inside interfaces:
Serial0
      Hits:0  Misses: 0
      .
```

路由器接口错误地定义成了 NAT 内部接口或 NAT 外部接口。

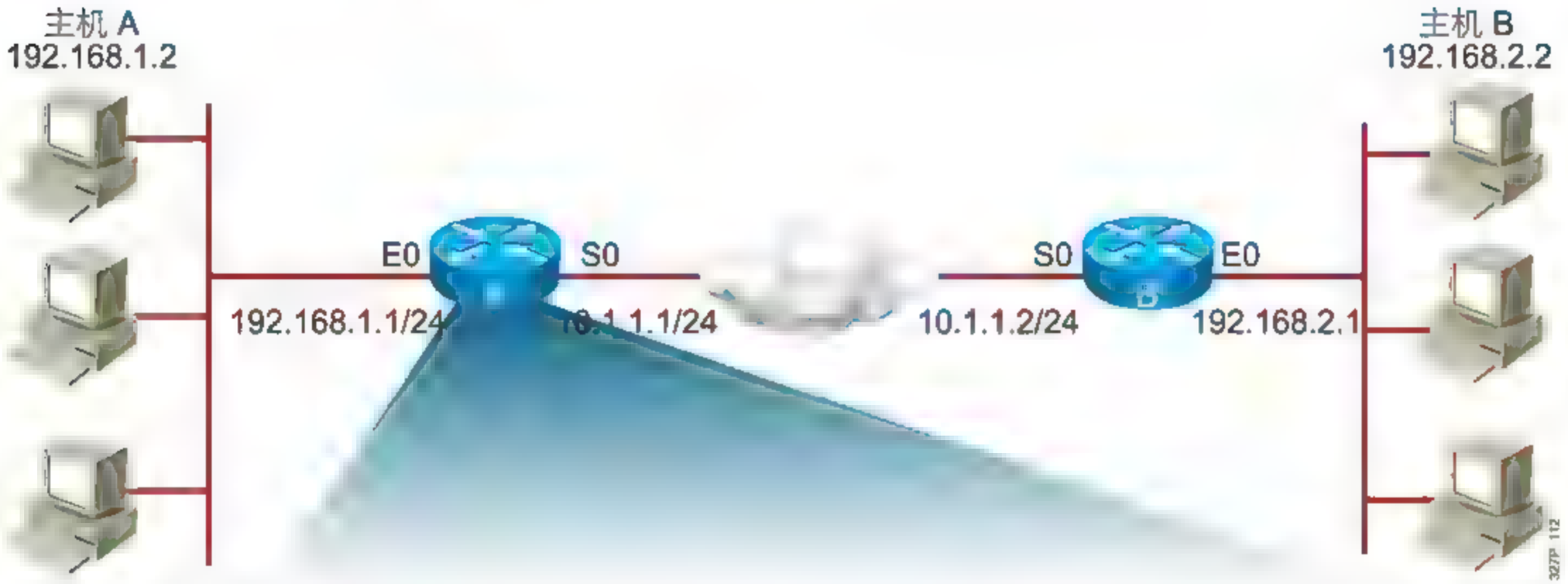
© 2008 Cisco Systems, Inc. 保留所有权利。

问题示例：无法 Ping 通远程主机（续）

```
RouterA# show access-list

Standard IP access list 20
  10 permit 0.0.0.0, wildcard bits 255.255.255.0
```

- Ping 仍然失败，转换表中仍没有转换。
- 在要定义哪些地址要转换的 ACL 中包含错误的通配符位掩码。

问题示例：无法 Ping 通远程主机（续）

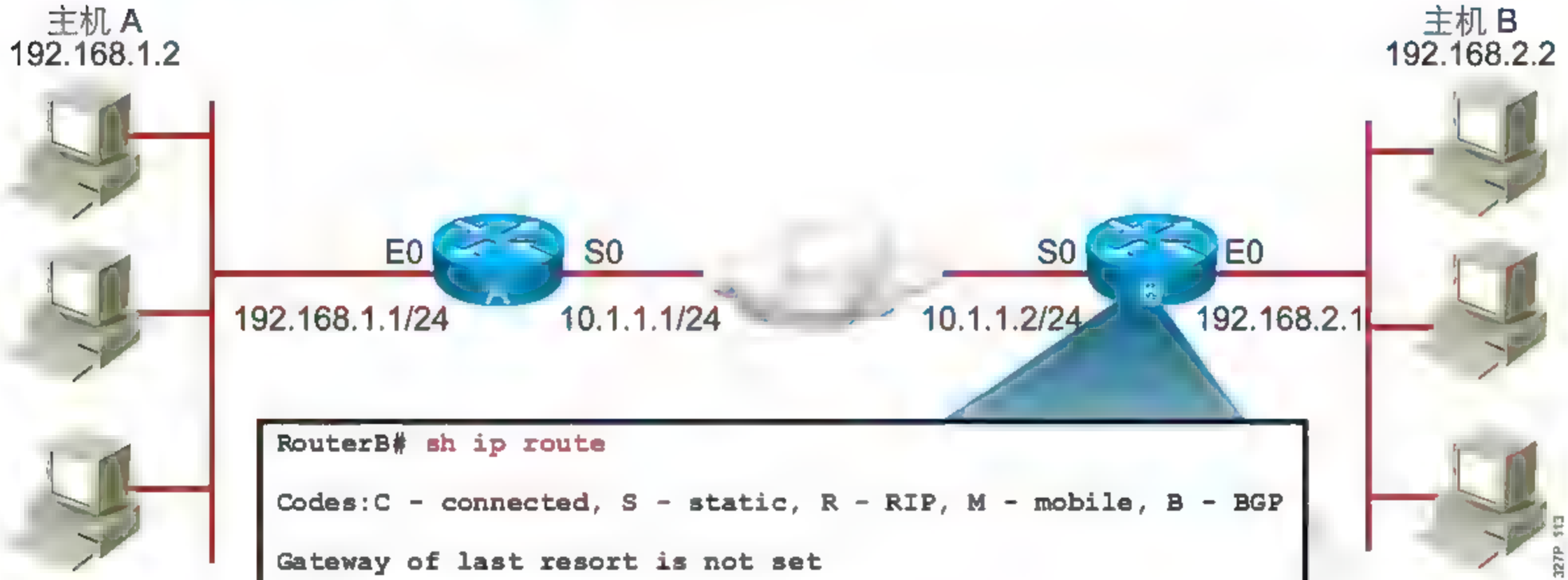



```
RouterA# show ip nat translations
      Pro Inside global      Inside local       Outside local      Outside global
      ---  172.16.17.20       192.168.1.2        ---                ---
```

- 转换现在可以执行。
- Ping 仍然失败。

© 2008 Cisco Systems, Inc. 保留所有权利。

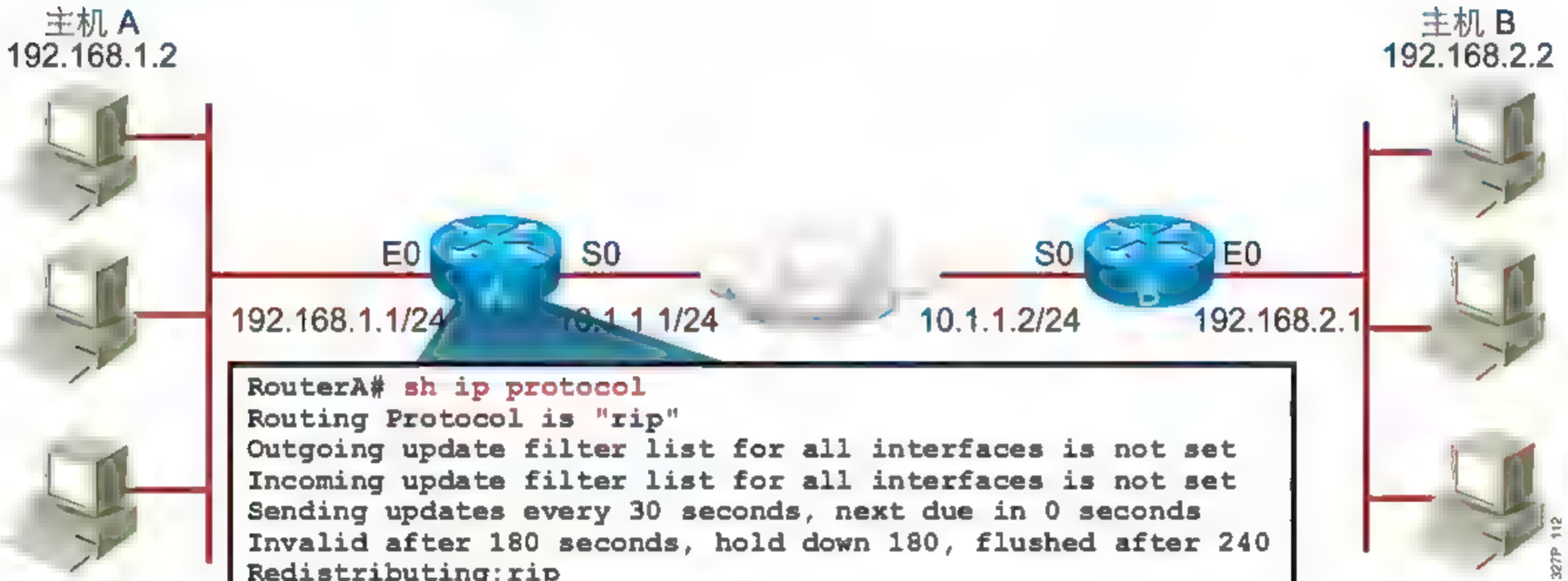
问题示例：无法 Ping 通远程主机（续）



路由器 B 上没有到转换后的网络地址 172.16.0.0 的路由。

Cisco Systems, Inc. 保留所有权利。

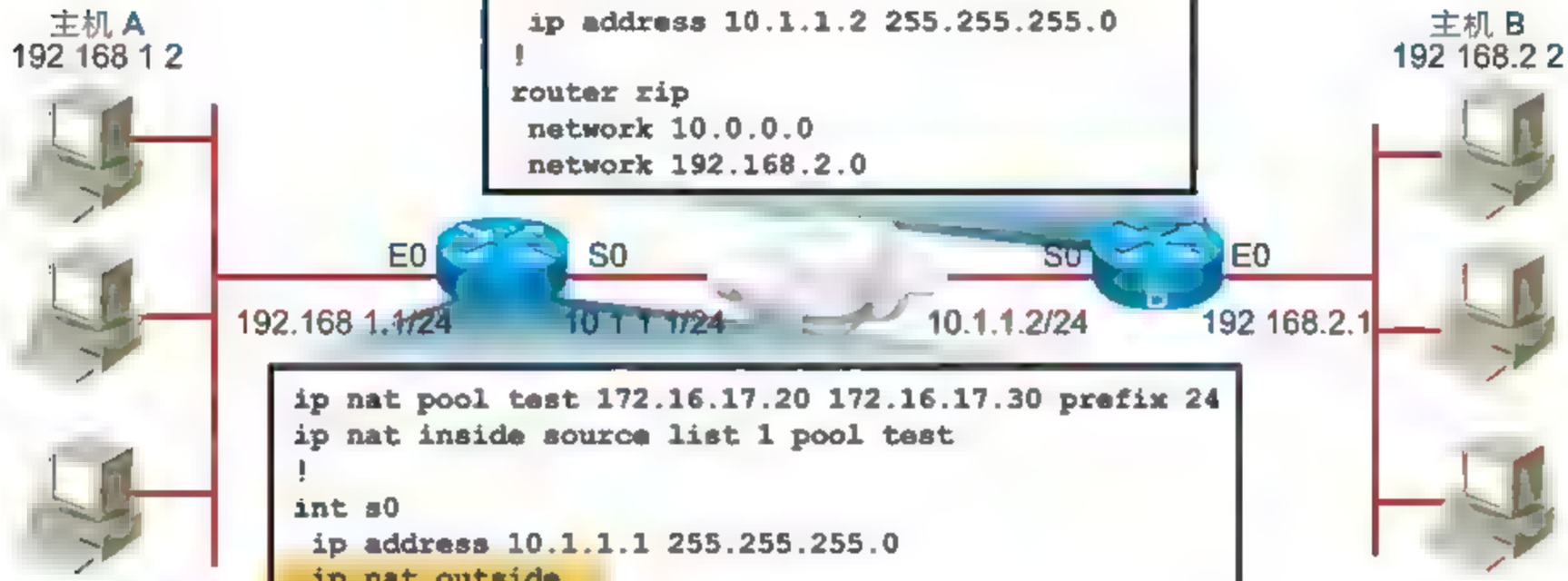
问题示例：无法 Ping 通远程主机（续）




```
RouterA# sh ip protocol
Routing Protocol is "rip"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Sending updates every 30 seconds, next due in 0 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Redistributing:rip
Default version control:send version 1, receive any version
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
    192.168.0.0
    10.0.0.0
Routing Information Sources:
Gateway         Distance      Last Update
Distance:(default is 120)
```

路由器 A 通告了要被转换的网络 192.168.1.0，
但没有通告路由器要被转换到的网络地址 172.16.0.0。

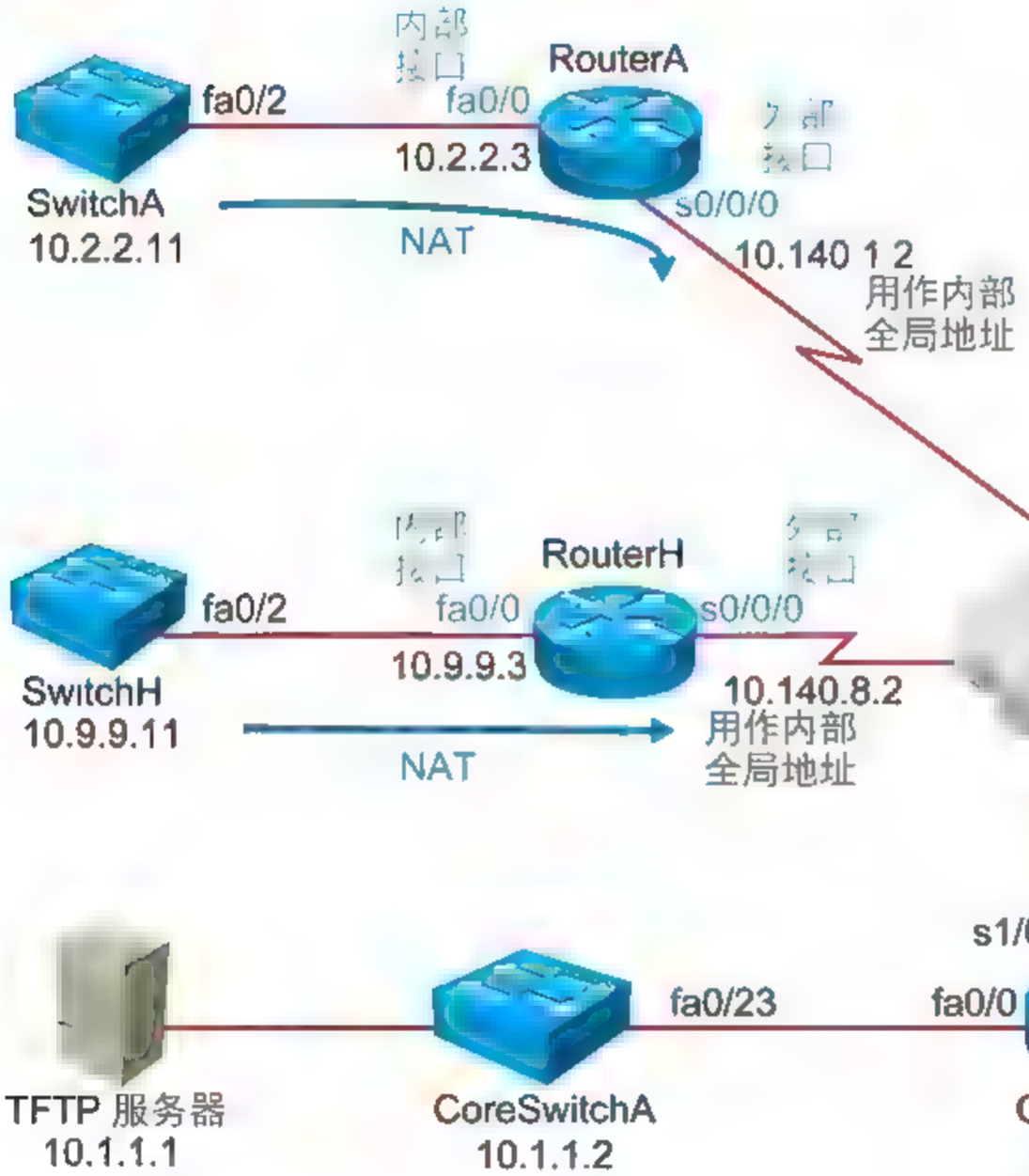
解決方案：正确的配置




```
int eo
 ip address 192.168.2.1 255.255.255.0
!
int s0
 ip address 10.1.1.2 255.255.255.0
!
router rip
 network 10.0.0.0
 network 192.168.2.0
```

```
ip nat pool test 172.16.17.20 172.16.17.30 prefix 24
ip nat inside source list 1 pool test
!
int s0
 ip address 10.1.1.1 255.255.255.0
 ip nat outside
!
int e0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
!
int loopback 0
 ip address 172.16.17.1 255.255.255.0
!
router rip
 network 10.0.0.0
 network 172.16.0.0
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

可视目标 7-1：配置 NAT 与 PAT



WG	路由器 s0/0/0	路由器 fa0/0	交换机
A	10.140.1.2	10.2.2.3	10.2.2.11
B	10.140.2.2	10.3.3.3	10.3.3.11
C	10.140.3.2	10.4.4.3	10.4.4.11
D	10.140.4.2	10.5.5.3	10.5.5.11
E	10.140.5.2	10.6.6.3	10.6.6.11
F	10.140.6.2	10.7.7.3	10.7.7.11
G	10.140.7.2	10.8.8.3	10.8.8.11
H	10.140.8.2	10.9.9.3	10.9.9.11

© 2008 Cisco Systems, Inc. 保留一切权利。

总结

- 有三类 NAT：静态、动态和过载 (PAT)。
- 静态 NAT 是一对一的地址映射。动态 NAT 地址是从地址池中挑选的。
- NAT 过载 (PAT) 允许将许多内部地址映射到一个外部地址。
- 使用 **show ip nat translation** 命令显示转换表，并检验是否发生转换。
- 要确定是否在使用当前转换条目，使用 **show ip nat statistics** 命令检查使用次数计数器。

CISCO

向 IPv6
过渡

地址空间管理

IPv4 和 IPv6

IPv4:	4 个二进制八位数
11000000.10101000.11001001.0111000	
192.168.201.113	
4,294,467,295 个 IP 地址	

- 目前大约有 13 亿可用的 IPv4 地址。

IPv6:	16 个二进制八位数
11010001.11011100.11001001.01110001.11010001.11011100. 11001100.01110001.11010001.11011100.11001001.01110001. 11010001.11011100.11001001.01110001	
A524:72D3:2C80:DD02:0029:EC7A:002B:EA73	
3.4 x 1038 个 IP 地址	

022P_152

© 2008 Cisco Systems, Inc. 保留所有权利。

为什么需要更大的地址空间？

- Internet 的人口
  - 2005 年 11 月大约有 9.73 亿用户
  - 新兴人口和地理地址空间
- 移动用户
  - PDA、平板电脑、笔记本电脑等
  - 2004 年大约 2000 万。
- 移动电话
  - 业界已交付 10 亿部移动电话
- 传输
  - 预计 2008 年将有 10 亿辆汽车
  - 在飞机上提供 Internet 接入服务，例如德国汉莎航空公司
- 消费者设备
  - Sony 强制要求到 2005 年为止，所有产品都必须支持 IPv6
  - 上亿的家用电器及工业电器

IPv6 高级功能

更大的地址空间：

- 全球连通性和灵活性
- 聚合
- 多源技术
- 自动配置
- 即插即用
- 无需 NAT 的端到端
- 重新编号

移动性和安全性：

- 与移动 IP RFC 兼容
- IPsec 强制用于（或自然用于）IPv6

更简单的报头：

- 路由效率
- 性能和转发速率的可扩展性
- 无广播
- 无校验和
- 扩展报头
- 流标签

多种过渡方式：

- 双协议栈
- 6to4 隧道和手动隧道
- 转换

IPv6 地址表示法

格式：

- x:x:x:x:x:x:x:x，其中 x 是 16 位的十六进制字段
  - 十六进制的 A、B、C、D、E 和 F 区分大小写
- 字段中的前导零是可选的
- 连续的零字段可表示为 ::每个地址只能用一次

示例：

- 2031:0000:130F:0000:0000:09C0:876A:130B
  - 可表示为 2031:0:130f::9c0:876a:130b
  - 不能表示为 2031::130f::9c0:876a:130b
- FF01:0:0:0:0:0:0:1 → FF01::1
- 0:0:0:0:0:0:0:1 → ::1
- 0:0:0:0:0:0:0:0 → ::

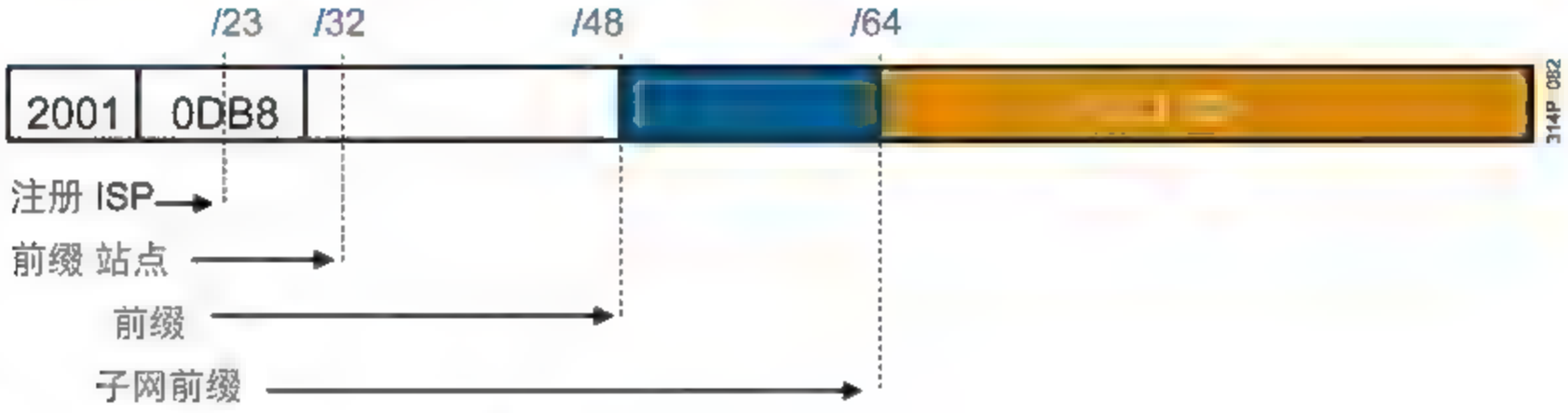
IPv6 地址类型

- 单播：
  - 地址用于单个接口
  - IPv6 有几种类型（例如，全局地址、保留地址、本地链路地址和本地站点地址）
- 组播：
  - 一对多
  - 提高网络的使用效率
  - 使用更大的地址范围
- 任播：
  - 一对最近（从单播地址空间分配）
  - 多个设备共享相同的地址
  - 所有任播节点应提供统一服务
  - 源设备将数据包发送到任播地址
  - 路由器确定最近的设备以达到目的地
  - 适合负载均衡和内容传输服务

IPv6 单播编址

- IPv6 单播地址类型：
  - 全局地址：以 2000::/3 开头，由 IANA 分配
  - 保留地址：由 IETF 使用
  - 私有地址：本地链路（以 FE80::/10 开头）
  - 环回地址 (::1)
  - 未指定地址 (::)
- 单个接口可分配多个任意类型的 IPv6 地址：单播、任播或组播。
- 多个 RFC 涵盖了 IPv6 编址规则。
  - 体系结构由 RFC 4291 定义

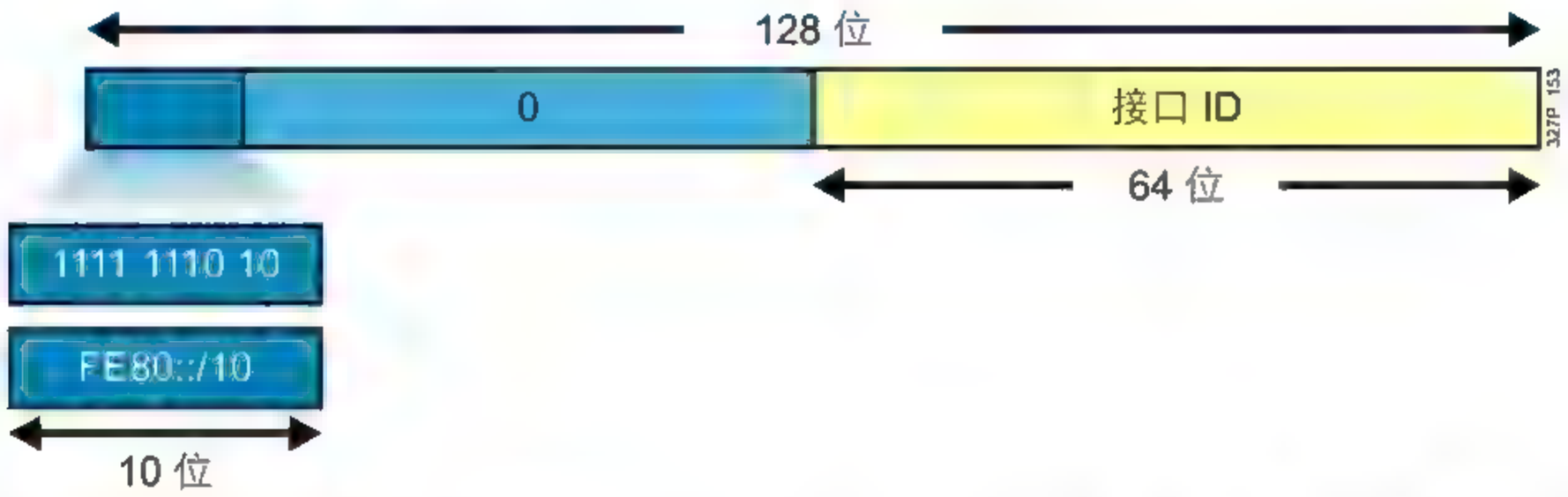
IPv6 全局单播（和任播）地址



IPv6 的全球单播地址和
任播地址的格式相同。

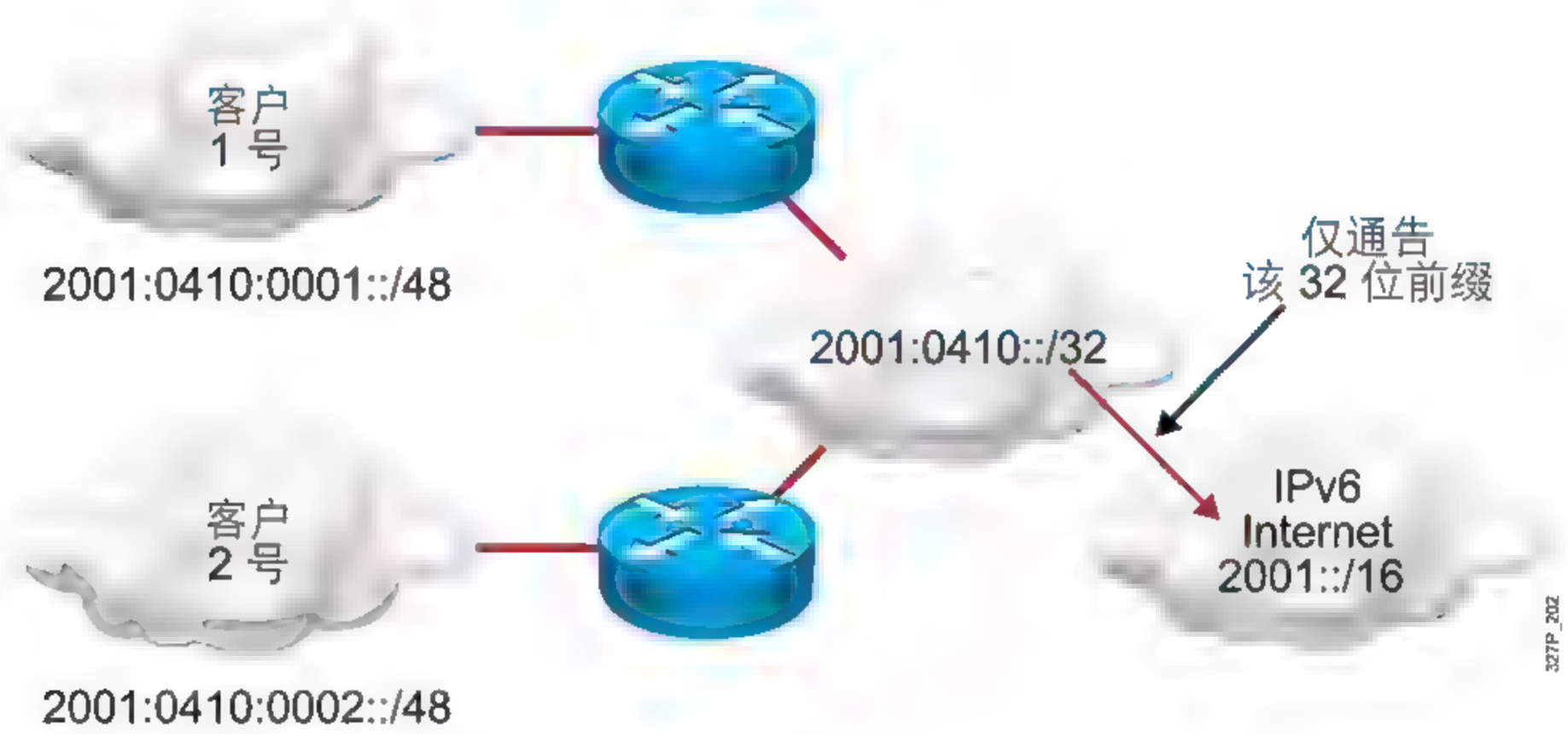
- 使用全球路由前缀，这是一种能向上聚合，最终到达 ISP 的结构。
- 单个接口可分配多个任意类型的地址（单播、任播、组播）。
- 每个支持 IPv6 的接口至少含有一个环回地址 (::1/128) 和一个本地链路地址。
- 每个接口可选择性地拥有多个唯一的本地地址和全球地址。

链路本地地址



- 本地链路地址的范围限制在链路之内，此地址在所有 IPv6 接口上通过使用指定的本地链路前缀 FE80::/10 和 64 位的接口标识符动态创建。
- 本地链路地址用于自动地址配置、邻居发现和路由器发现。很多路由协议也使用本地链路地址。
- 本地链路地址可连接相同本地网络中的设备，而且无需全球地址。
- 使用本地链路地址通信时，因每个接口都连接到 FE80::/10，所以必须指定传出接口。

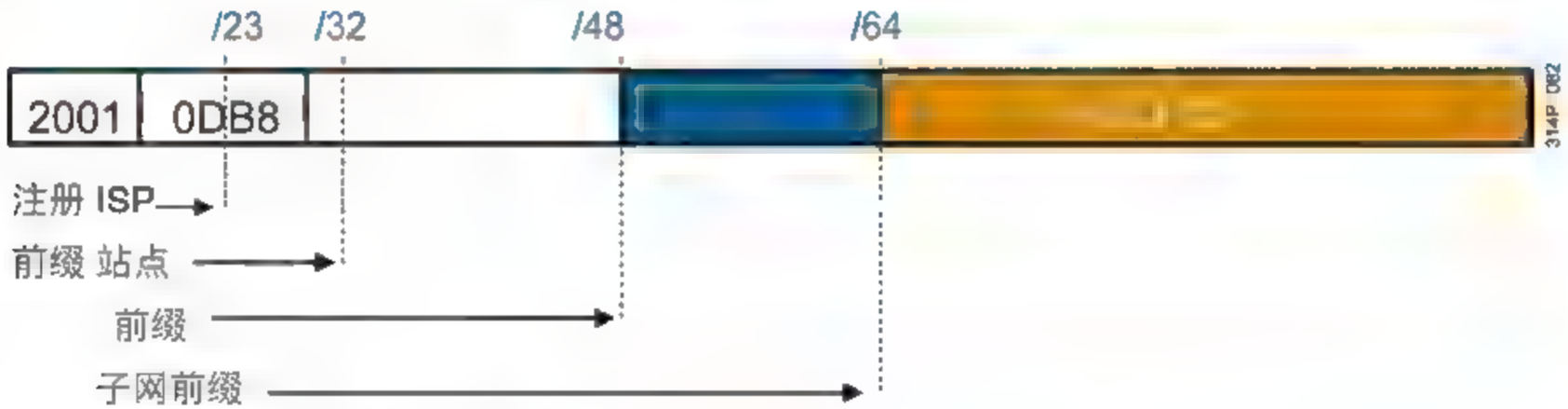
更大的地址空间可进行地址聚合



地址聚合具有以下优点：

- 聚合全球路由表中通告的前缀
- 路由有效且可以扩展
- 提高用户流量的带宽和功能性

分配 IPv6 全球单播地址



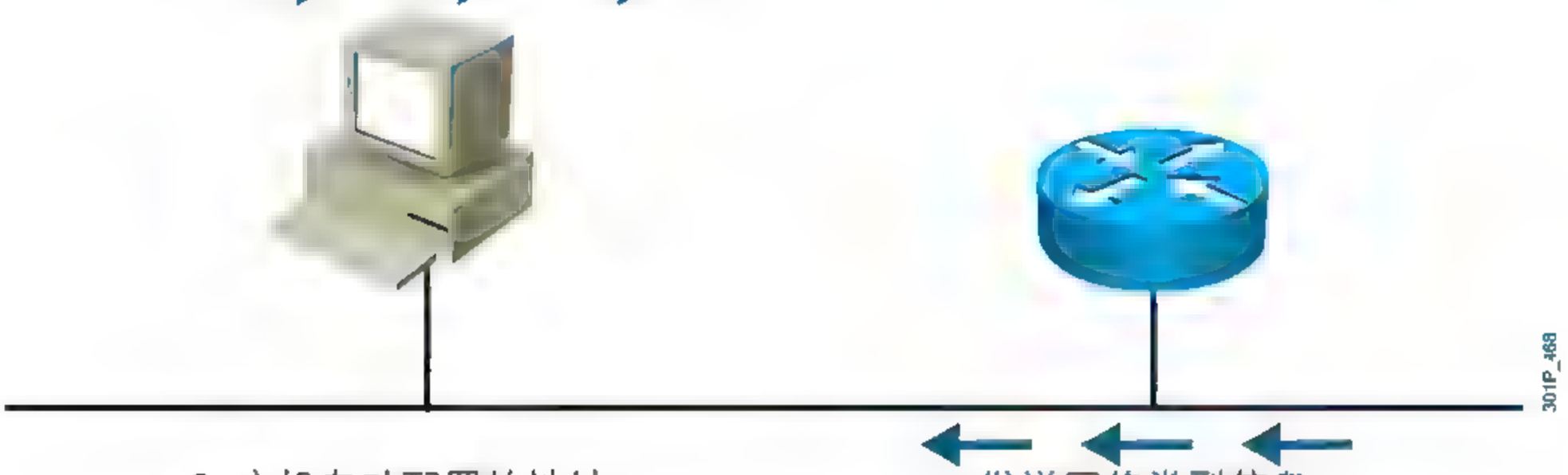
- 静态分配
  - 手动接口 ID 分配
  - EUI-64 接口 ID 分配
- 动态分配
  - 无状态自动配置
  - DHCPv6（全状态）

IPv6 EUI-64 接口标识符

- Cisco 可使用 EUI-64 格式的接口标识符。
- 此格式向中间的 16 位插入“FFFE”以将 48 位的 MAC 地址扩展为 64 位。
- 为表示所选地址来自唯一的以太网 MAC 地址，全球范围的 U/L 位设置为 1（本地范围的 U/L 位则设置为 0）。

无状态自动配置

1. 路由器请求
申请前缀



3. 主机自动配置的地址：
接收到的前缀 + 链路层地址

发送网络类型信息
(前缀、默认路由 ...)
2. 路由器通告

DHCPv6（全状态）

DHCPv6 是 IPv4 的 DHCP 更新版本：

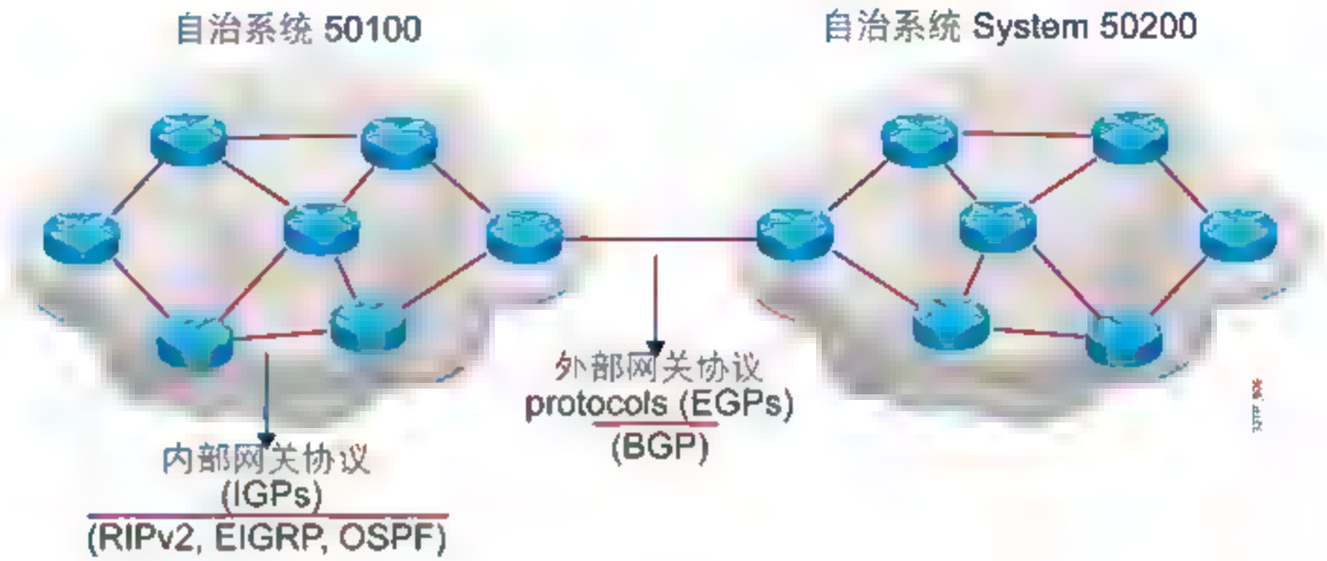
- 支持新的编址
- 启用了比无状态自动配置更多的控制
- 可用于重新编号
- 可用于为使用动态 DNS 的主机进行自动域名注册

DHCPv6 操作

DHCPv6 的操作方式与 DHCPv4 类似，除了：

- 客户端首先检测链路上是否存在路由器。
- 如果发现路由器，则检查路由器通告，确定是否可使用 DHCP。
- 如果没发现路由器，或如果路由器可以使用 DHCP，则：
  - 将 DHCP 请求消息发送到“全 DHCP 代理”组播地址。
  - 客户端将本地链路地址用作源地址。

IPv6 路由协议



- IPv6 路由类型：
  - 静态
  - RIPng (RFC 2080)
  - OSPFv3 (RFC 2740)
    - 用于 IPv6 的 IS-IS
  - MP-BGP4 (RFC 2545/2858)
  - 用于 IPv6 的 EIGRP
- 配置任何路由协议之前，需要使用 **ipv6 unicast-routing** 命令来启用 IPv6。

RIPng (RFC 2080)

与 IPv4 相似的功能：

- 距离矢量、15 跳的半径、水平分割和毒性反转
- 基于 RIPv2

IPv6 的更新功能：

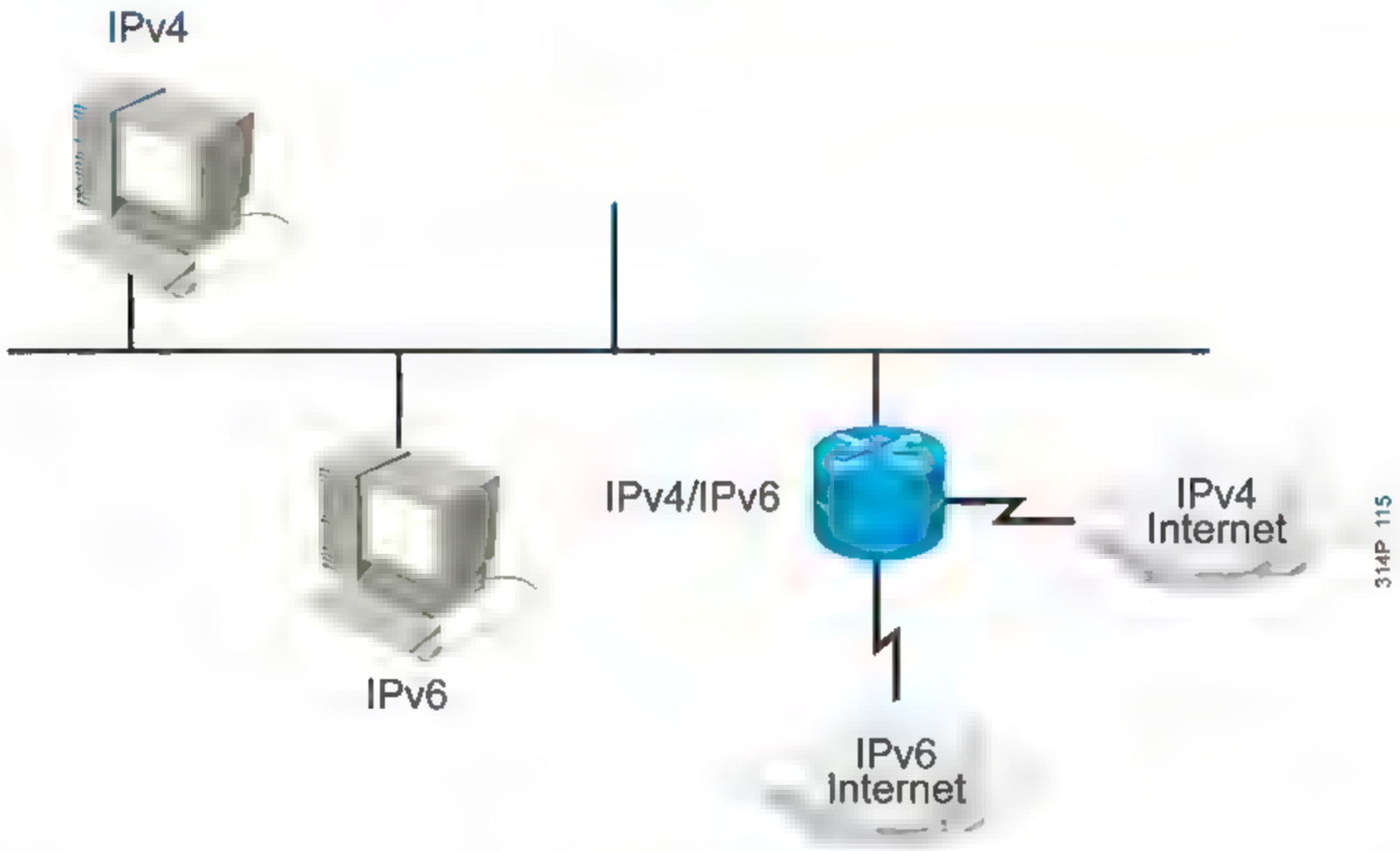
- IPv6 前缀、下一跳 IPv6 地址
- 使用组播组 FF02::9（全 RIP 路由器组播组）作为 RIP 更新的目的地址
- 使用 IPv6 传输数据
- 命名的 RIPng

IPv4 向 IPv6 过渡

具有多种过渡方式，这表示：

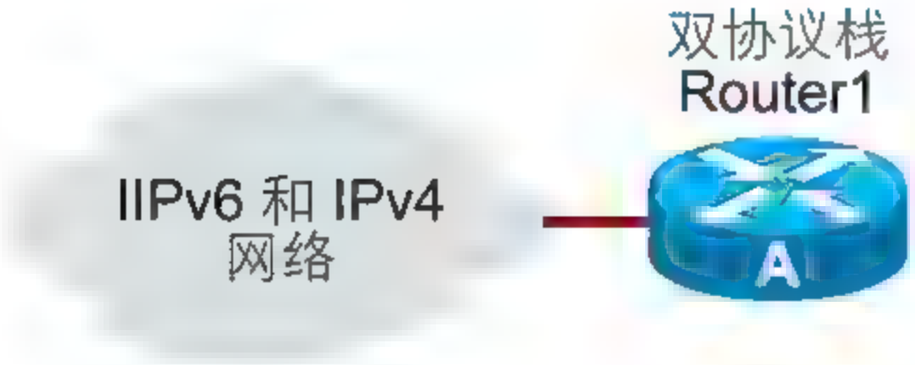
- 没有固定的转换日期；不需要立刻对所有地址进行转换
- 有不同的过渡机制可用：
  - 双协议栈
  - 手动隧道
  - 6to4 隧道
  - ISATAP 隧道
  - Teredo 隧道
- 不同的兼容机制：
  - 代理和转换 (NAT-PT)

Cisco IOS 双协议栈



双协议栈是一种集成方法，使用这种方法时，节点可以同时实施和连通 IPv4 网络与 IPv6 网络。

Cisco IOS 双协议栈（续）



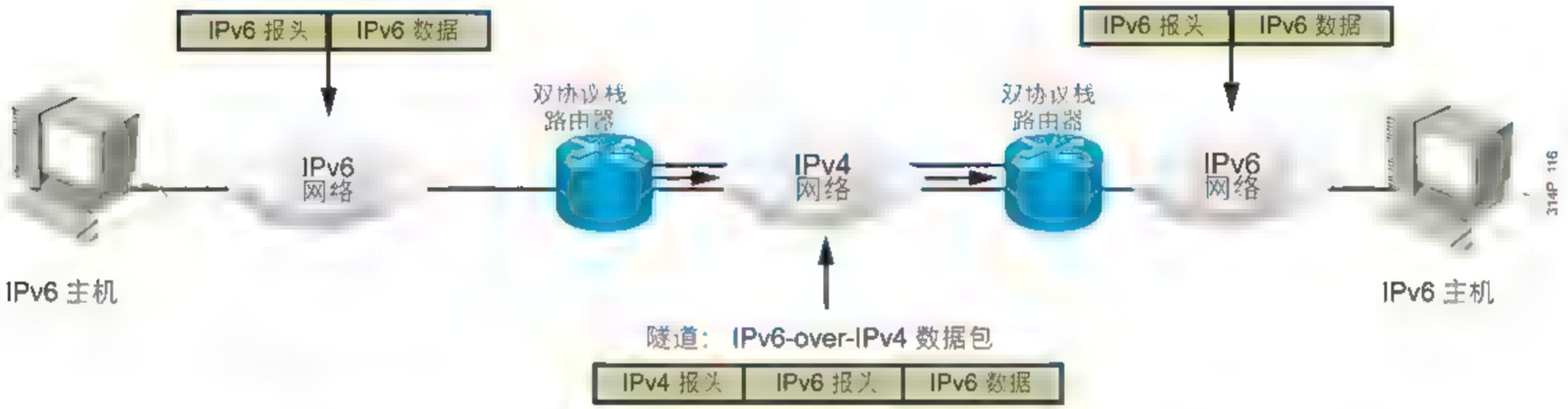

```
conf t
ipv6 unicast-routing

interface ethernet0
 ip address 192.168.99.1 255.255.255.0
 ipv6 address 3ffe:b00:c18:1::3/127
```

IPv4: 192.168.99.1
IPv6: 3ffe:b00:c18:1::3

327P_141

如果在一个接口上同时配置 IPv4 和 IPv6，则可将该接口视为双协议栈接口。

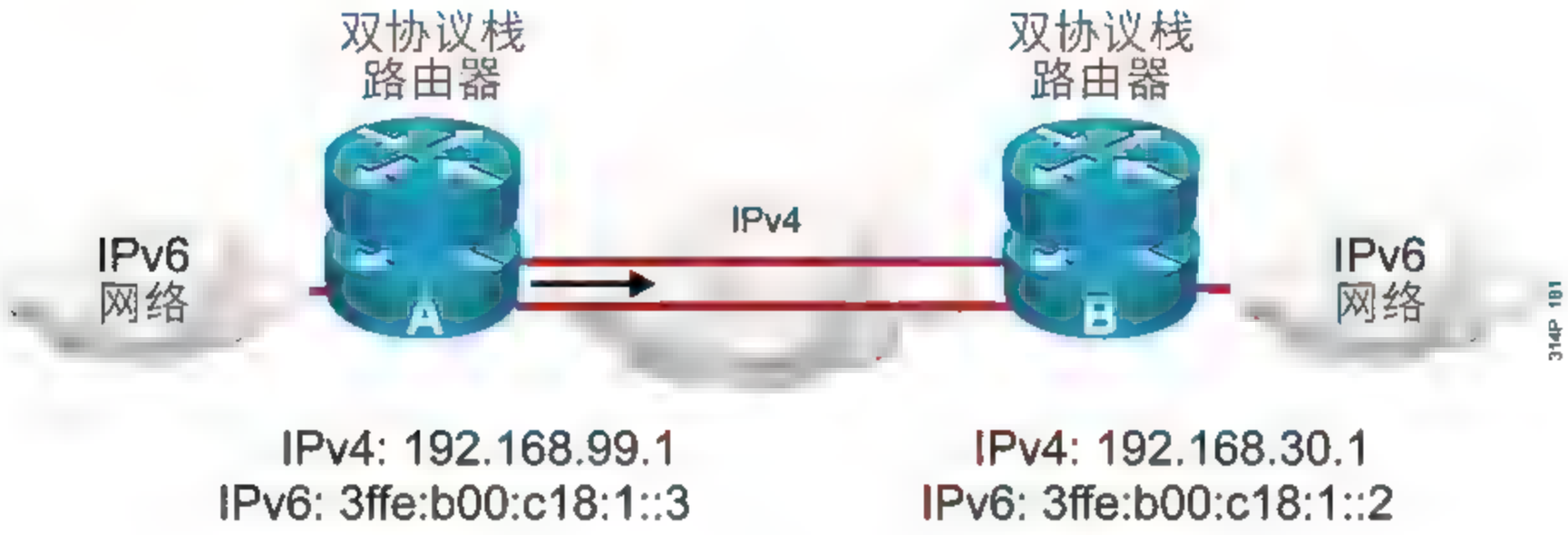
IPv6 隧道技术



隧道是一种集成方法，使用这种方法时，IPv6 数据包将被封装在另一种协议中，例如 IPv4。此封装方法是 IPv4。

- 数据包含有一个不带选项的 20 字节 IPv4 报头、一个 IPv6 报头及负载
- 数据包需要使用双协议栈路由器

手动配置 IPv6 隧道



配置隧道时需要：

- 两端具备双协议栈
- 每一端上均配置 IPv4 和 IPv6 地址

© 2008 Cisco Systems, Inc. 保留所有权利。

在 Cisco 路由器上启用 IPv6

```
RouterX(config)#
ipv6 unicast-routing
```

- 启用 IPv6 流量转发

```
RouterX(config-if)#
ipv6 address ipv6prefix/prefix-length [eui-64]
```

- 配置接口 IPv6 地址

IPv6 地址配置示例

LAN: 2001:db8:c18:1::/64

Ethernet 0

```
ipv6 unicast-routing
interface Ethernet0
 ipv6 address 2001:db8:c18:1::/64 eui-64
```

MAC 地址：0060.3e47.1530

```
RouterX# show ipv6 interface Ethernet0
Ethernet0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::260:3EFF:FE47:1530
Global unicast address(es):
    2001:DB8:C18:1:260:3EFF:FE47:1530, subnet is 2001:DB8:C18:1::/64
  Joined group address(es):
    FF02::1:FF47:1530
    FF02::1
    FF02::2
  MTU is 1500 bytes
```

327P_108

Cisco IOS IPv6 域名解析

Cisco IOS IPv6 域名解析有两种方法：

- 为 IPv6 地址定义静态名称

```
RouterX(config)#
ipv6 host name [port] ipv6addr [{ipv6addr} ...]
```

```
RouterX(config)# ipv6 host router1 3ffe:b00:ffff:b::1
```

- 配置一台或多台 DNS 服务器以供查询

```
RouterX(config)#
ip name-server address
```

```
RouterX(config)#ip name-server 3ffe:b00:ffff:1::10
```

配置和检验 IPv6 的 RIPng

RouterX(config)#

```
ipv6 router rip tag
```

- 创建并进入 RIP 路由器配置模式

RouterX(config-if)#

```
ipv6 rip tag enable
```

- 在接口上配置 RIP

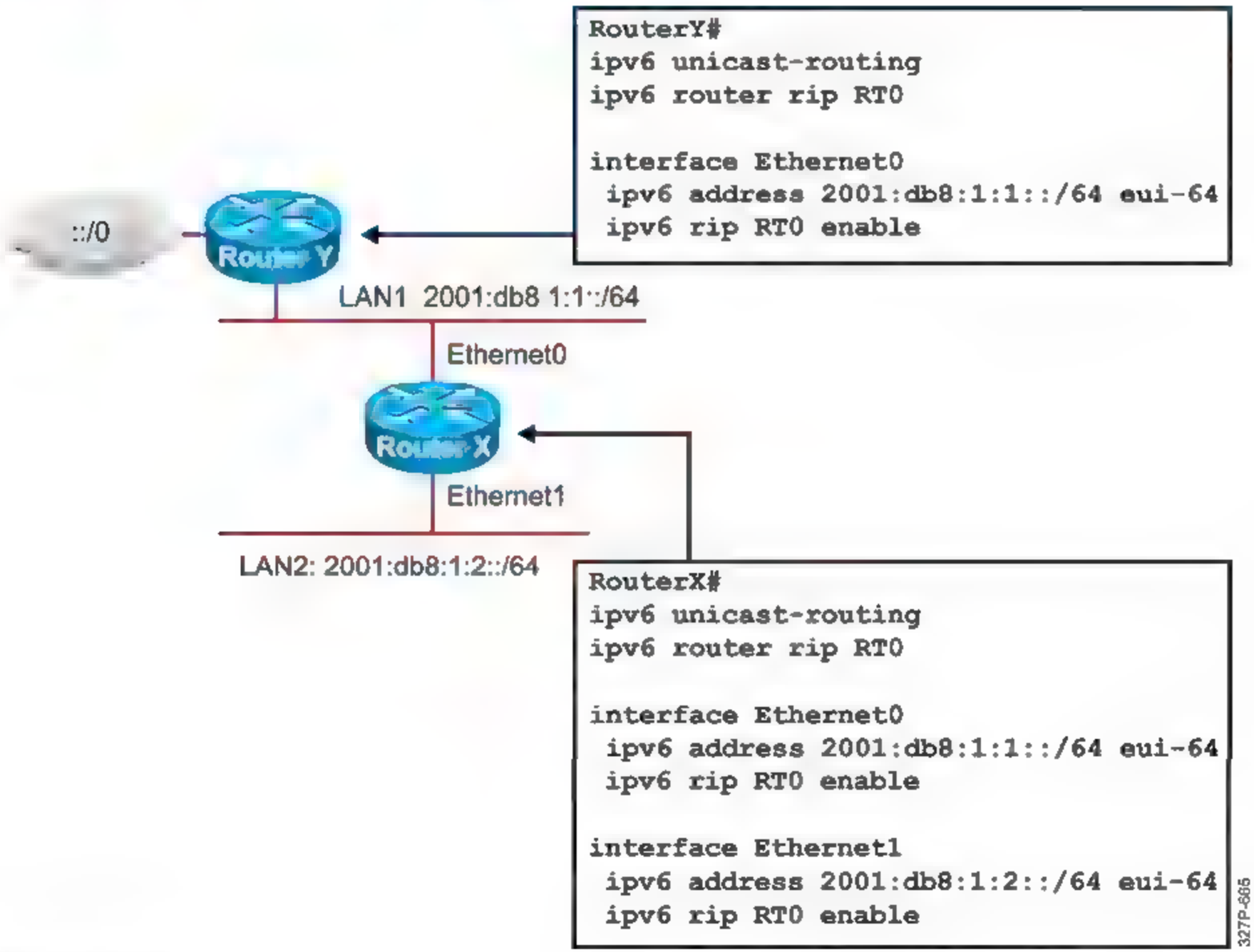
```
show ipv6 rip
```

- 显示各种 RIP 进程的状态

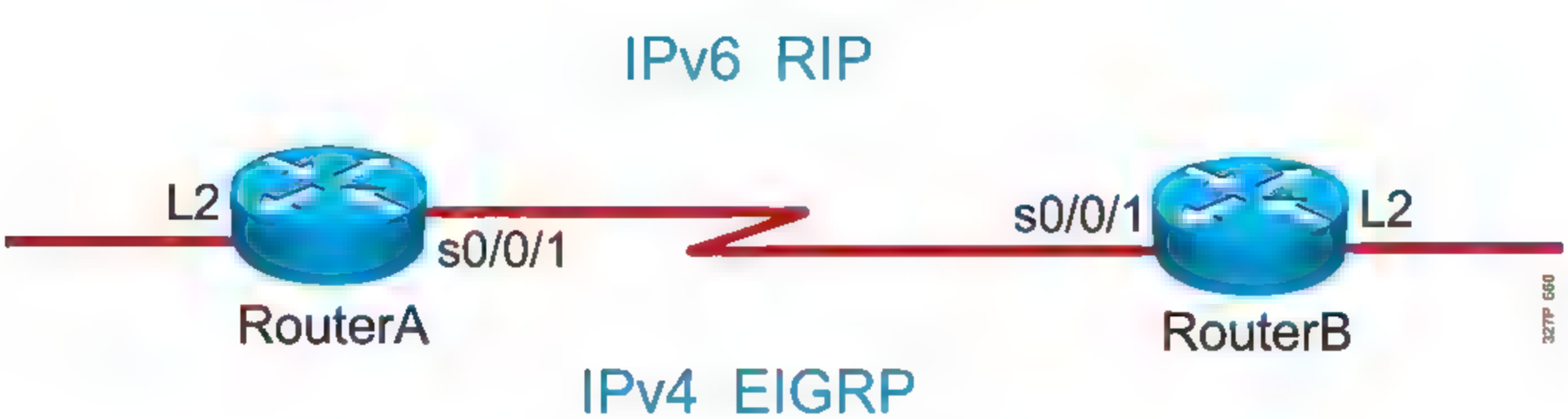
```
show ipv6 route rip
```

- 显示 IPv6 路由表中的 RIP 路由

IPv6 的 RIPng 配置实例



可视目标 7-2：实施 IPv6



总结

- IPv6 比 IPv4 具有更多的优势，包括更大的地址空间、更容易的地址聚合和集成安全性。
- IPv6 地址的长度为 128 位，由 48 位的全局前缀、16 位的子网 ID 和 64 位的接口标识符组成。
- 可使用多种方式分配 IPv6 地址：静态、无状态自动配置和 DHCPv6。
- Cisco 支持所有主要的 IPv6 路由协议：RIPng、OSPFv3 和 EIGRP。
- 从 IPv4 过渡到 IPv6 需要使用双协议栈、隧道，还可能需要 NAT-PT。
- 使用 **ipv6 unicast-routing** 命令启用 IPv6，使用 **ipv6 address** *ipv6-address/prefix-length* 命令分配接口地址并启用 IPv6 路由协议。

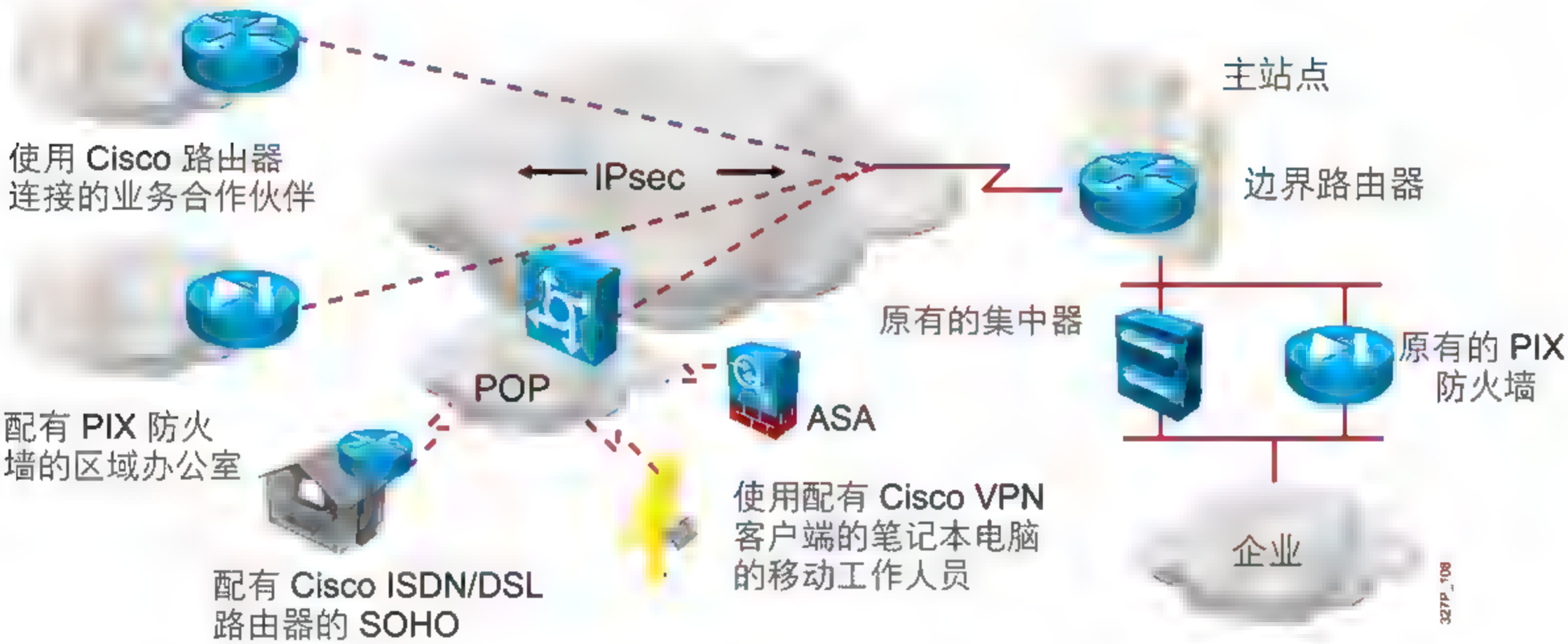
单元总结

- 对于 IPv4 所提供的数量有限的唯一 IP 地址而言，NAT 是一种短期解决方案。可配置的 NAT 类型包括静态、动态和过载 (PAT)。
- 而 IPv6 则是应对 IPv4 地址即将耗尽的长期解决方案。IPv6 将 IP 地址的大小增加为 128 位，并包含了自动配置、安全性等多种功能以及多个从 IPv4 过渡到 IPv6 的解决方案。

VPN 解决方案简介

LAN 延伸到 WAN

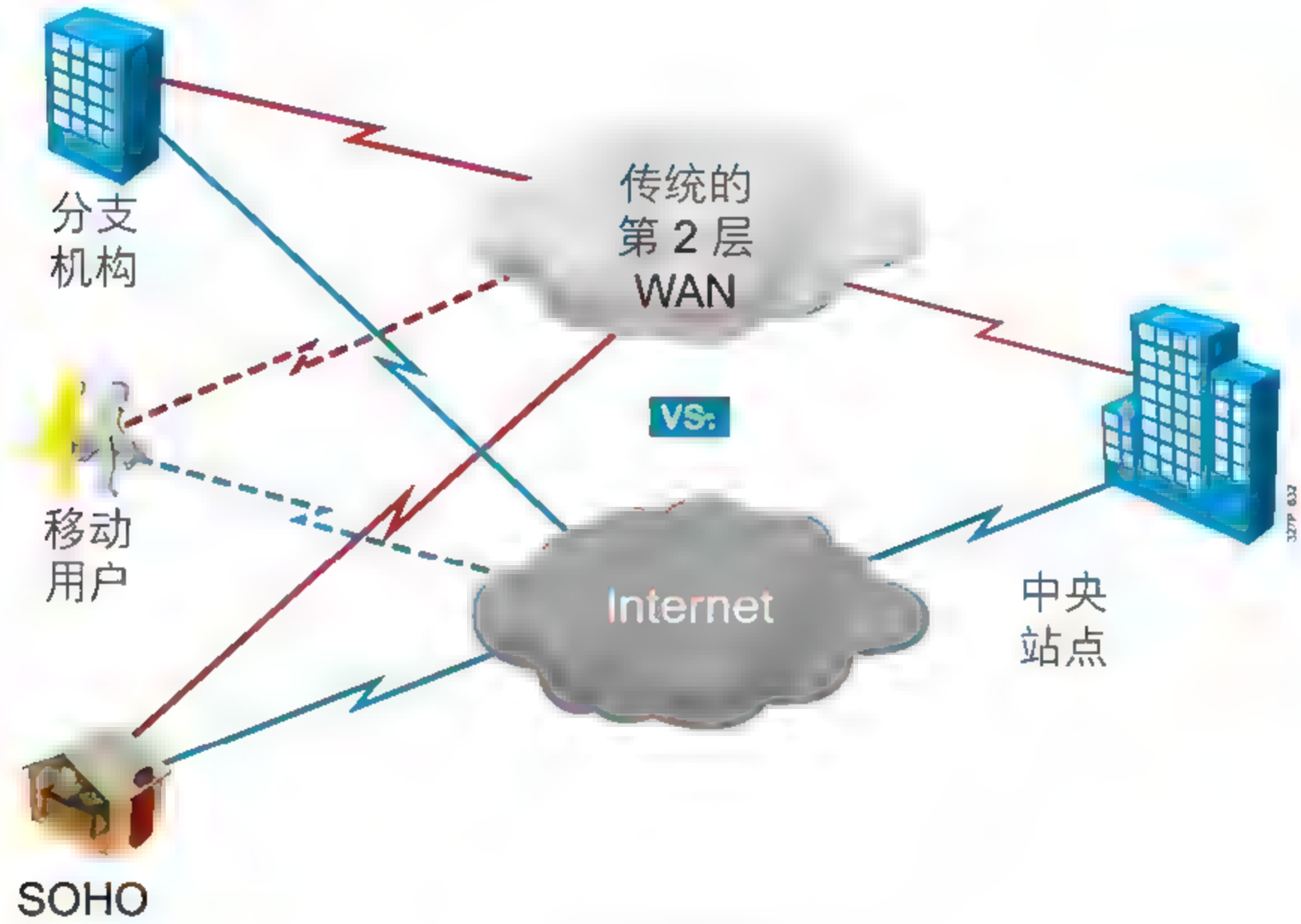
什么是 VPN？



虚拟：私有网络中的信息通过公共网络传输。

私有：对流量进行加密以保持数据的机密性。

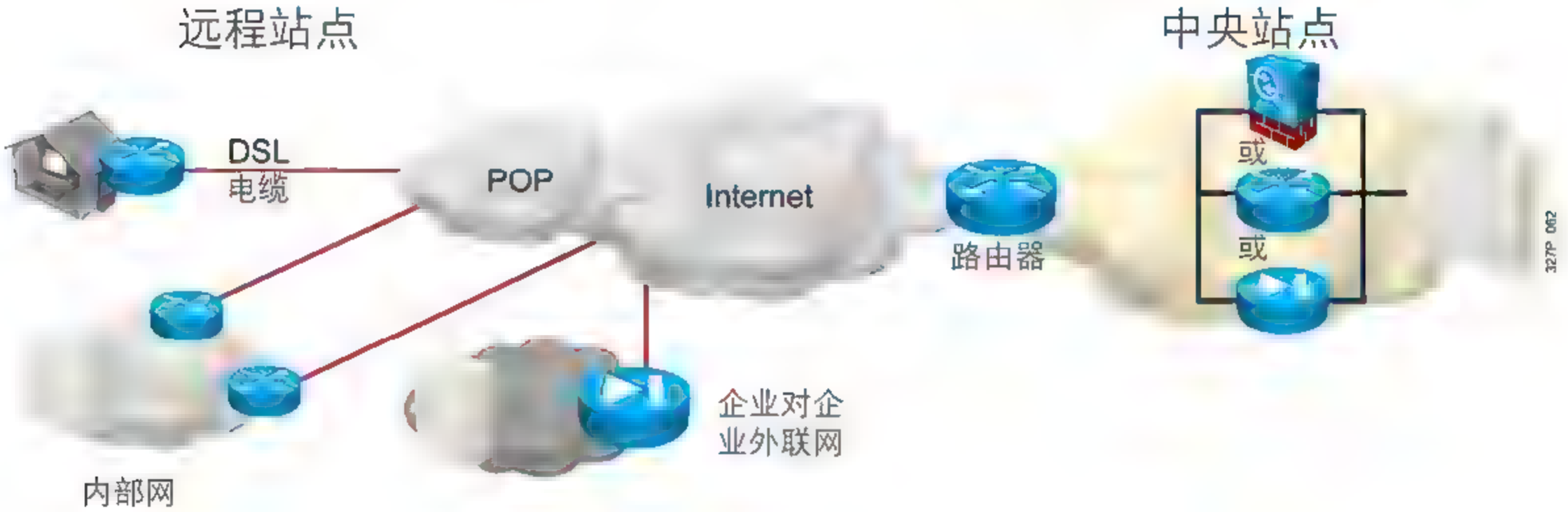
VPN 的优点



- 可扩展性

© 2008 Cisco Systems, Inc. 保留所有权利。

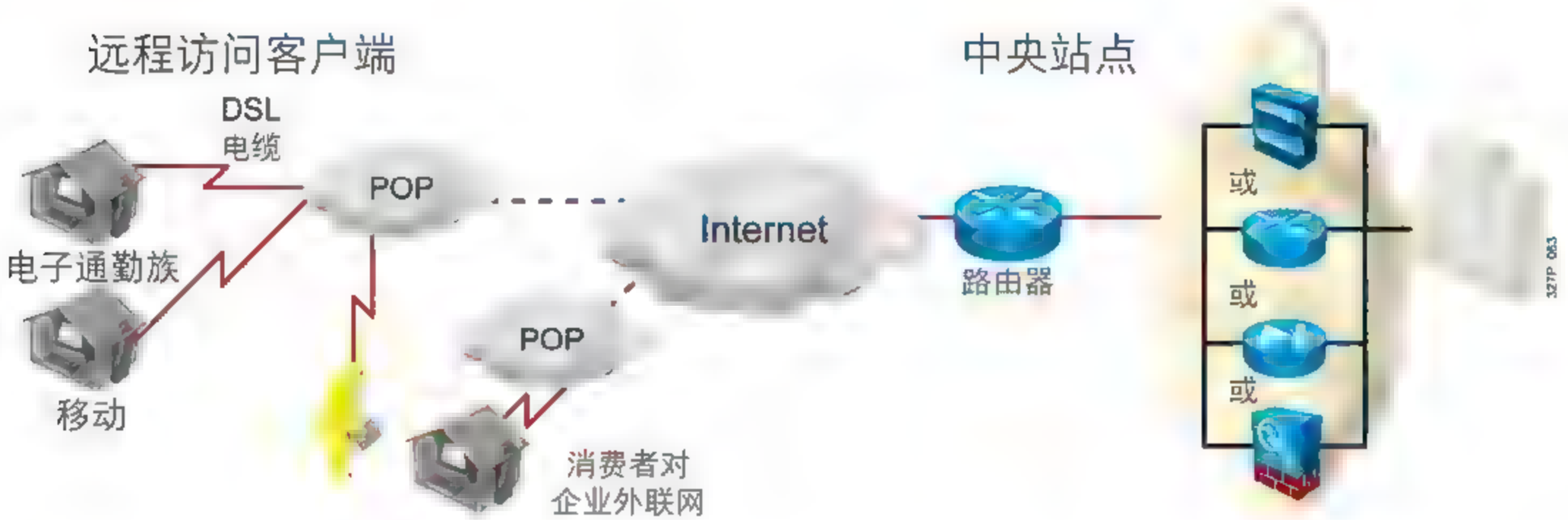
站点间 VPN



站点间 VPN：传统 WAN 的扩展

© 2008 Cisco Systems, Inc. 保留所有权利。

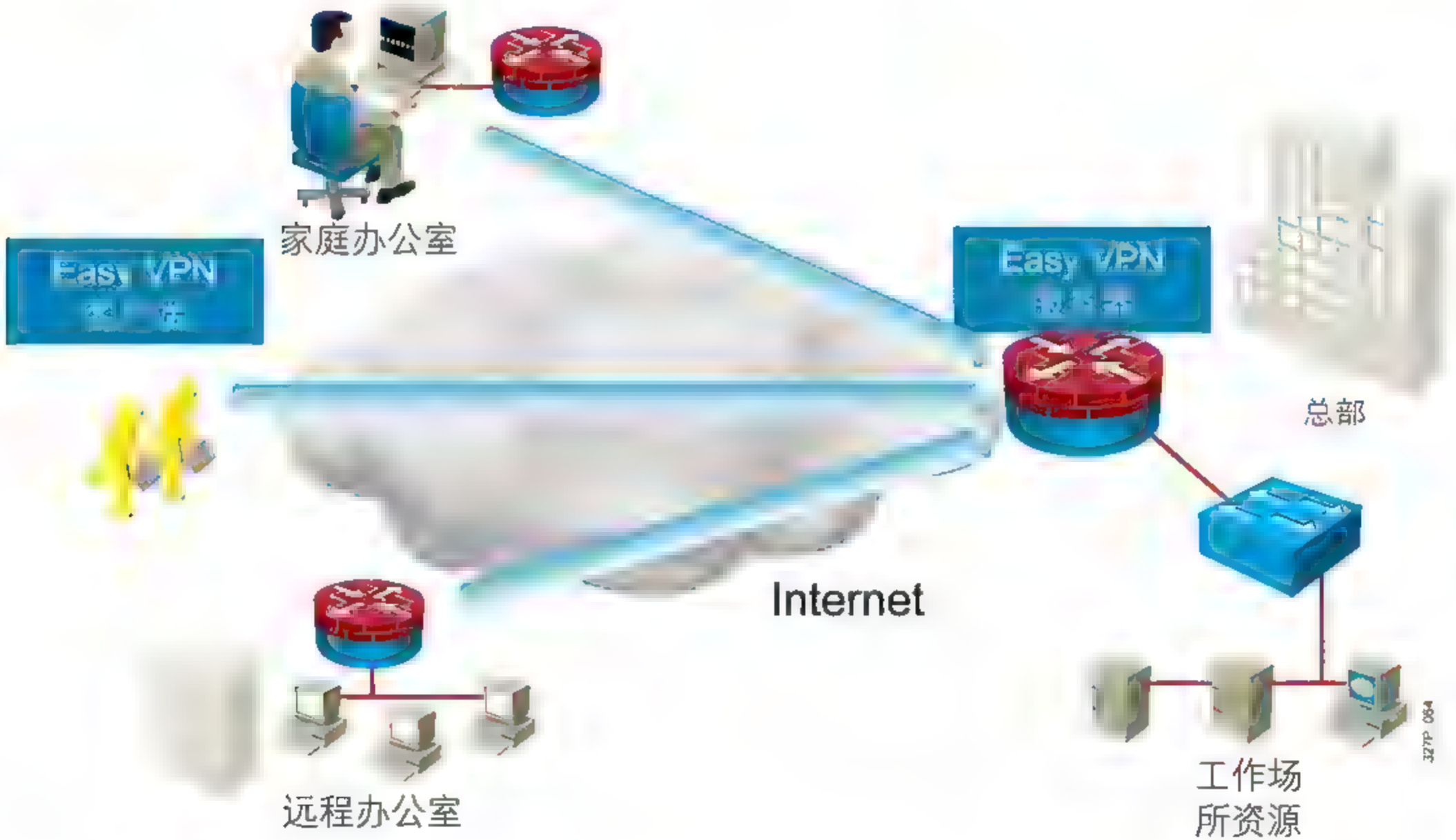
远程访问 VPN



远程访问 VPN：拨号网络和 ISDN 的发展

© 2008 Cisco Systems, Inc. 保留所有权利。

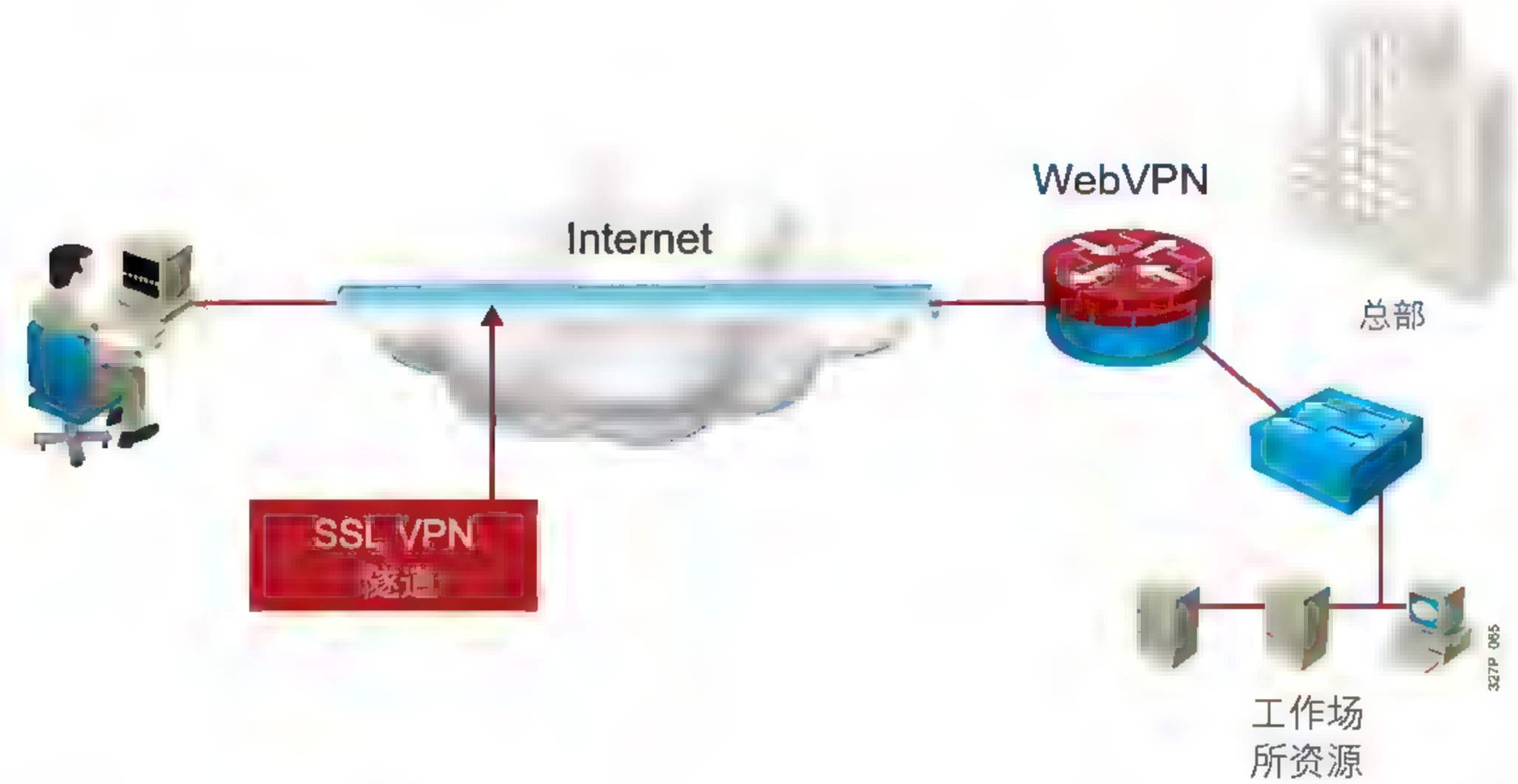
Cisco Easy VPN



© 2008 Cisco Systems, Inc. 保留所有权利。

Cisco IOS IPsec SSL VPN (WebVPN)

- 集成安全性和路由



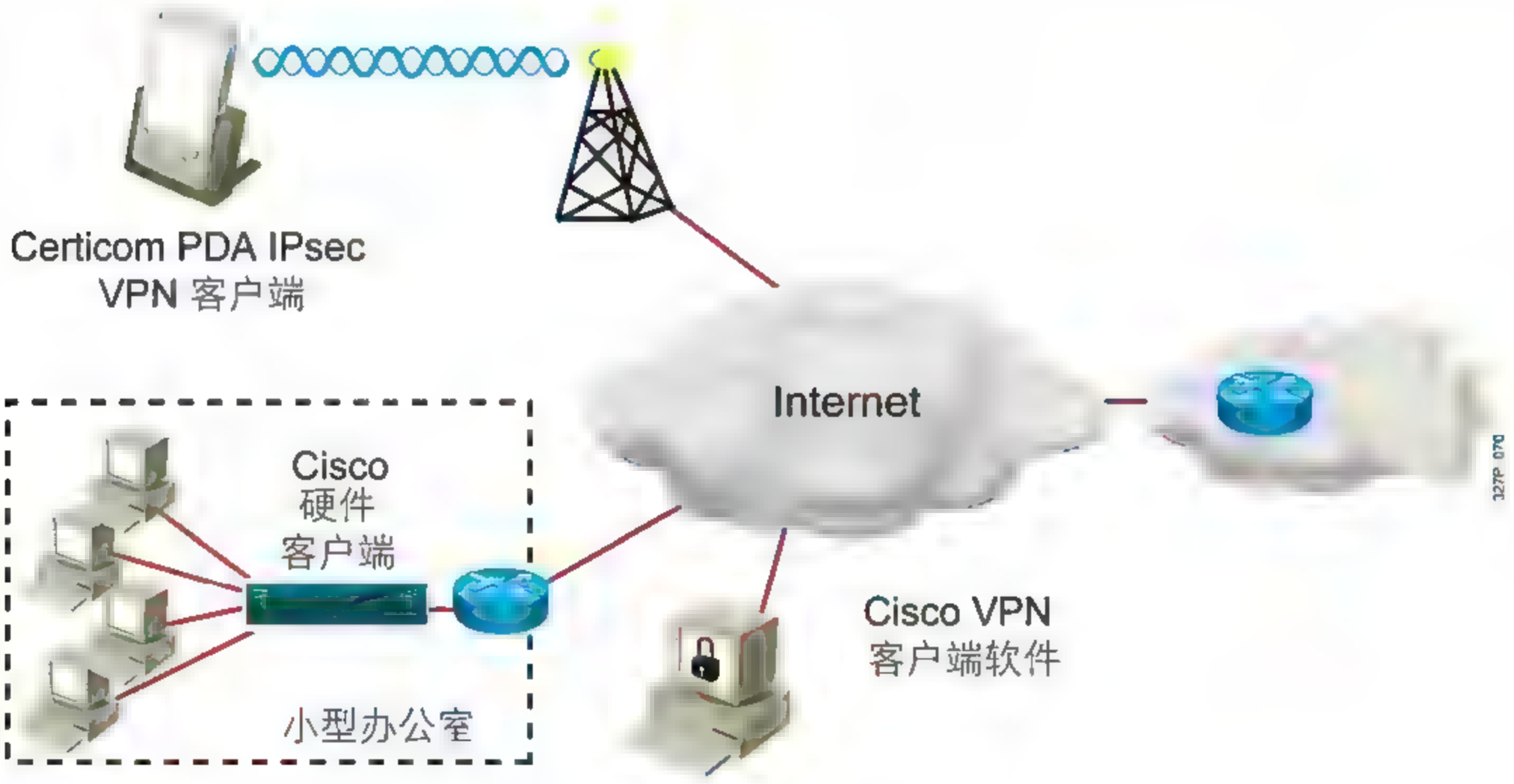
支持 VPN 的 Cisco IOS 路由器

© 2008 Cisco Systems, Inc. 保留所有权利。

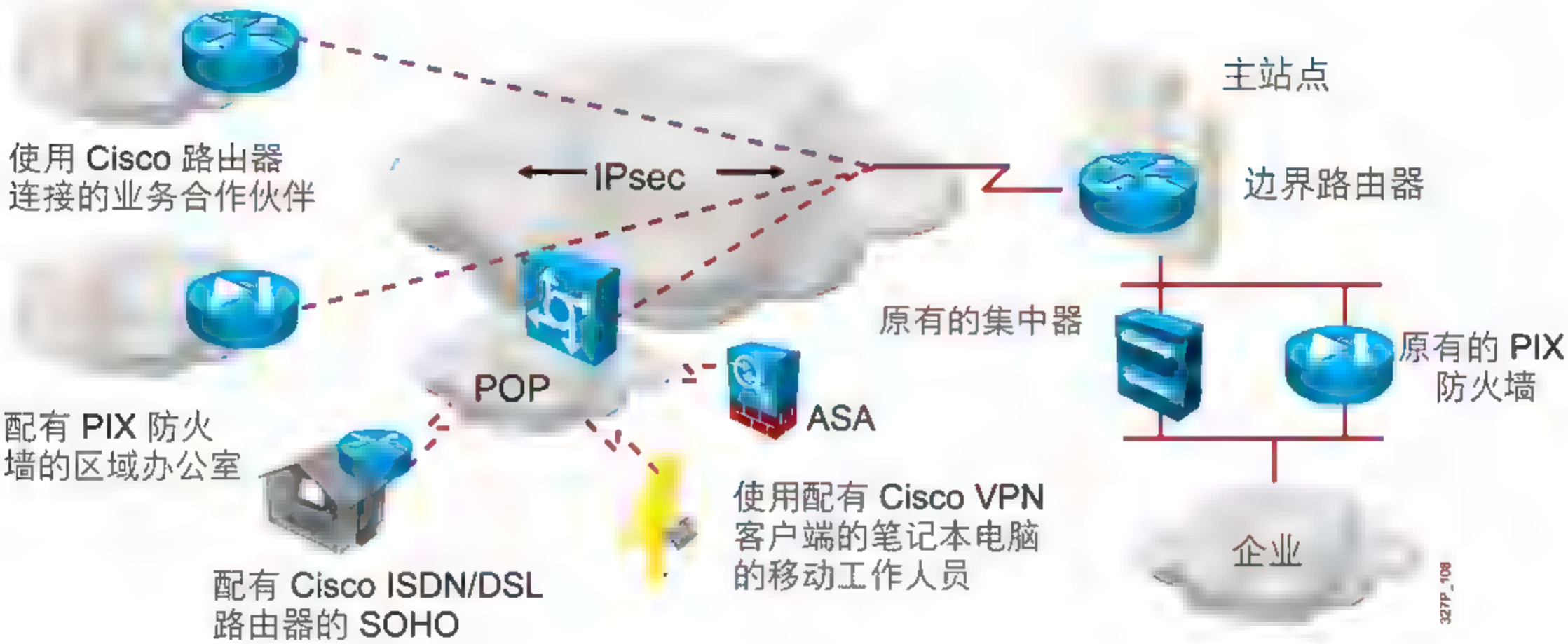
Cisco ASA 自适应安全设备

© 2008 Cisco Systems, Inc. 保留所有权利。

VPN 客户端


Certicom PDA IPsec
VPN 客户端
Internet
Cisco
硬件
客户端
小型办公室
Cisco VPN
客户端软件

什么是 IPsec？



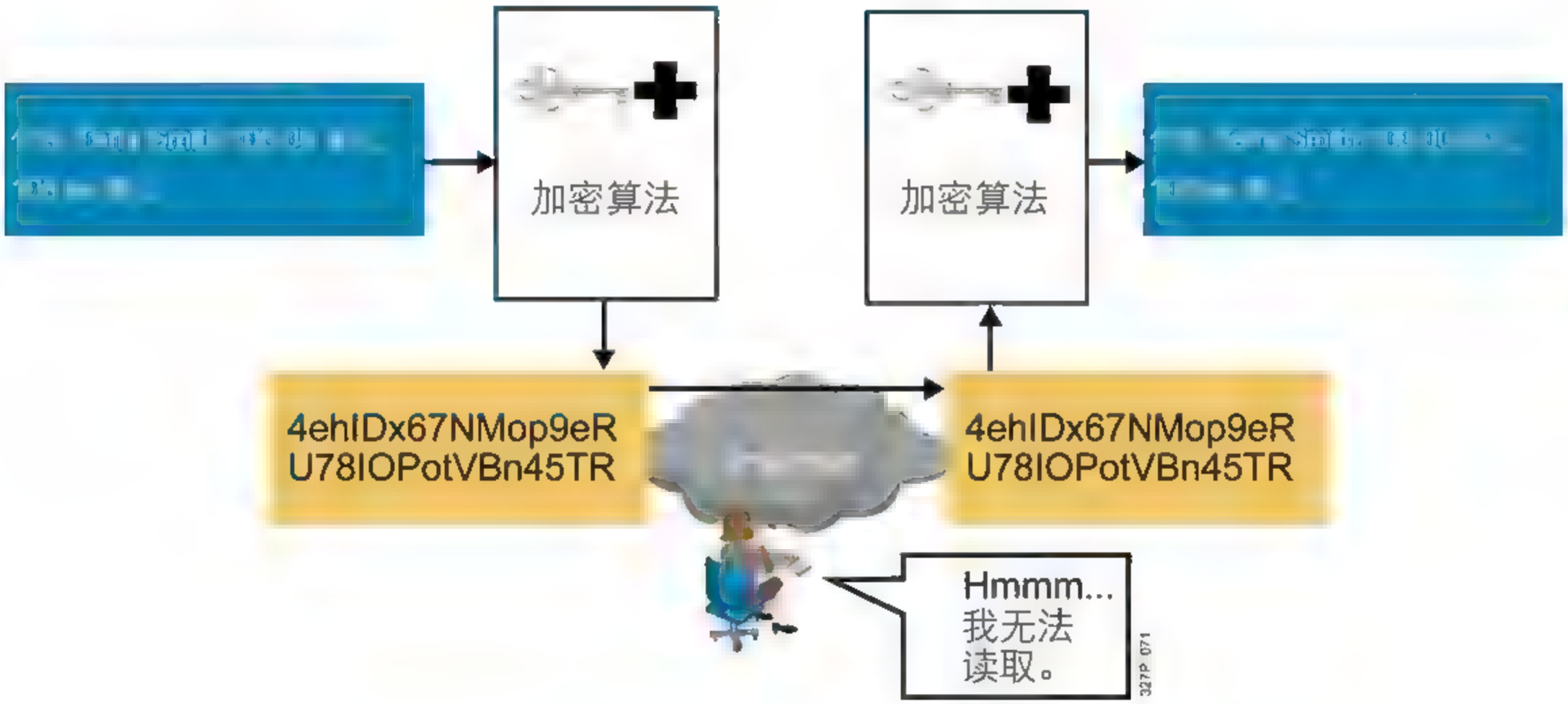
IPsec 在网络层起作用，保护和验证 IP 数据包。

- 它是一种与算法无关的开放式标准框架。
- 而且它提供数据机密性、数据完整性和来源验证。

IPsec 安全服务

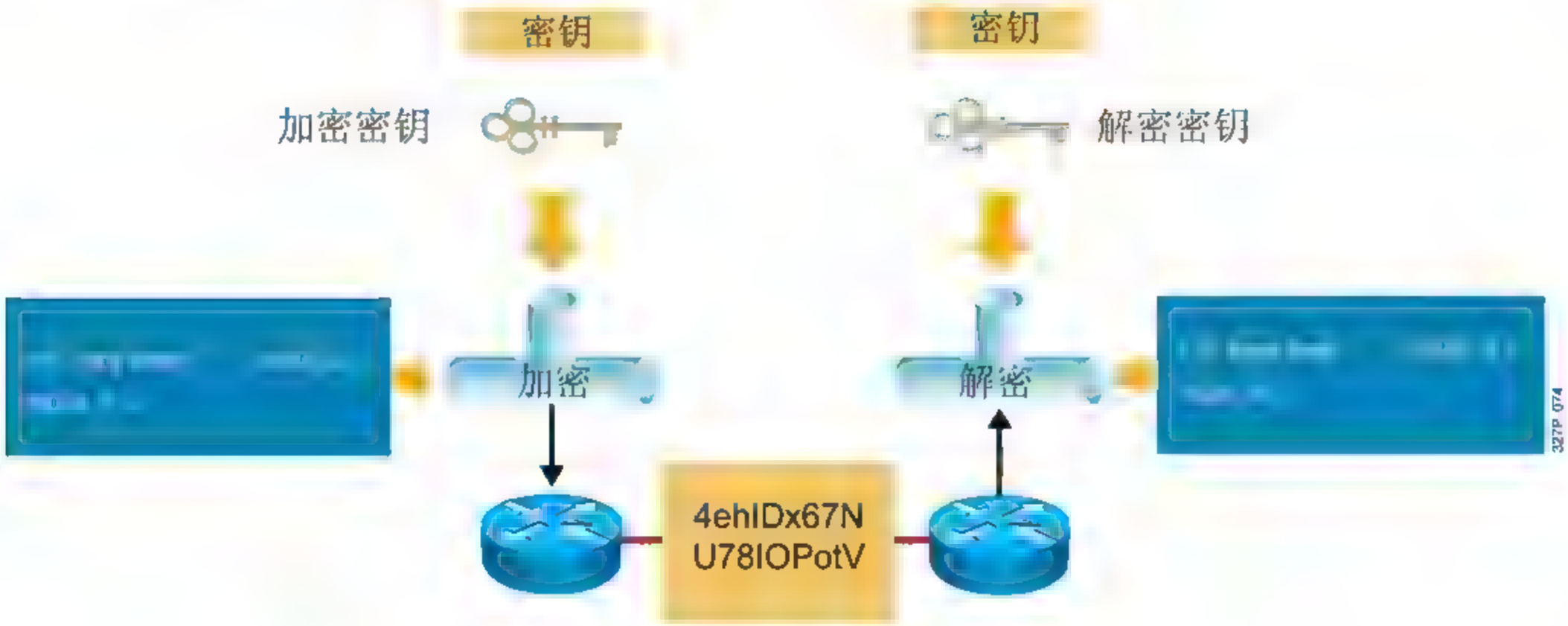
- 机密性
- 数据完整性
- 身份验证
- 反重播保护

机密性（加密）



© 2008 Cisco Systems, Inc. 保留所有权利。

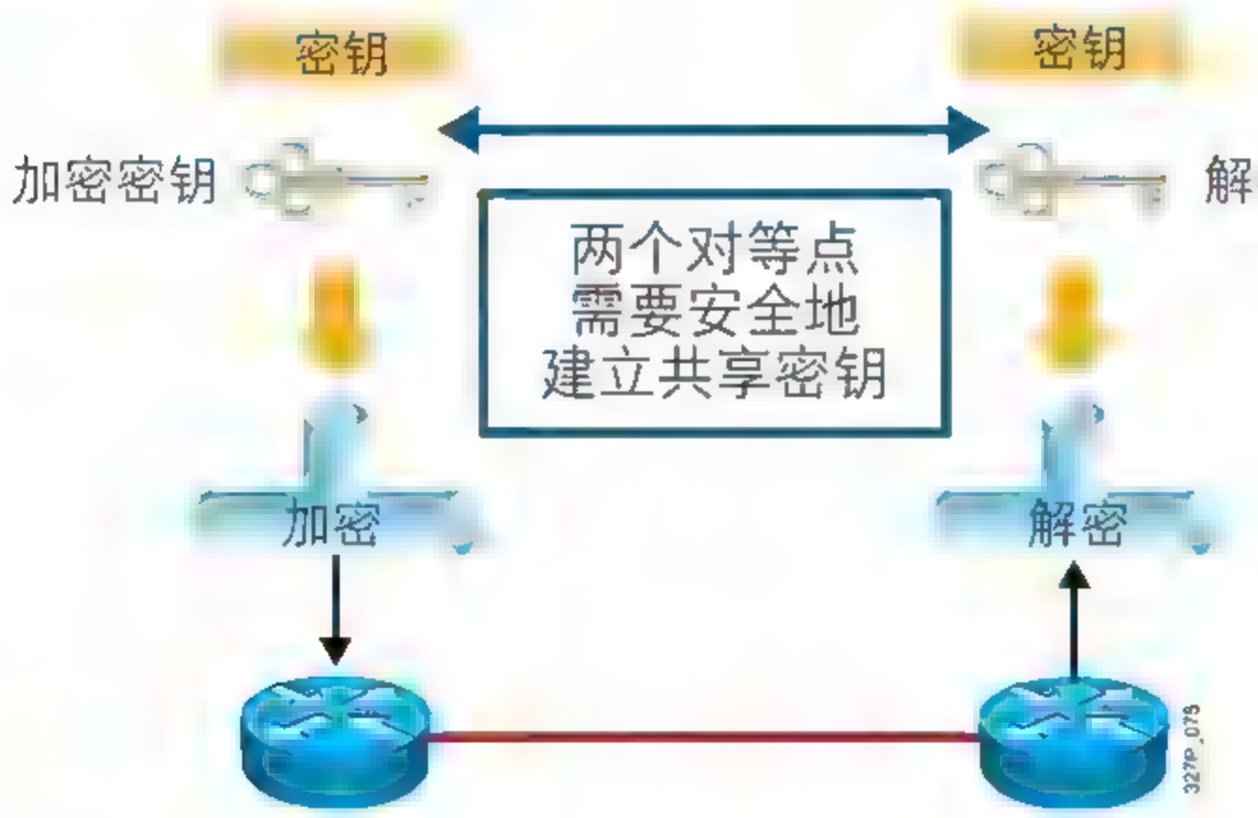
加密算法



加密算法：

- DES
- 3DES
- AES
- RSA

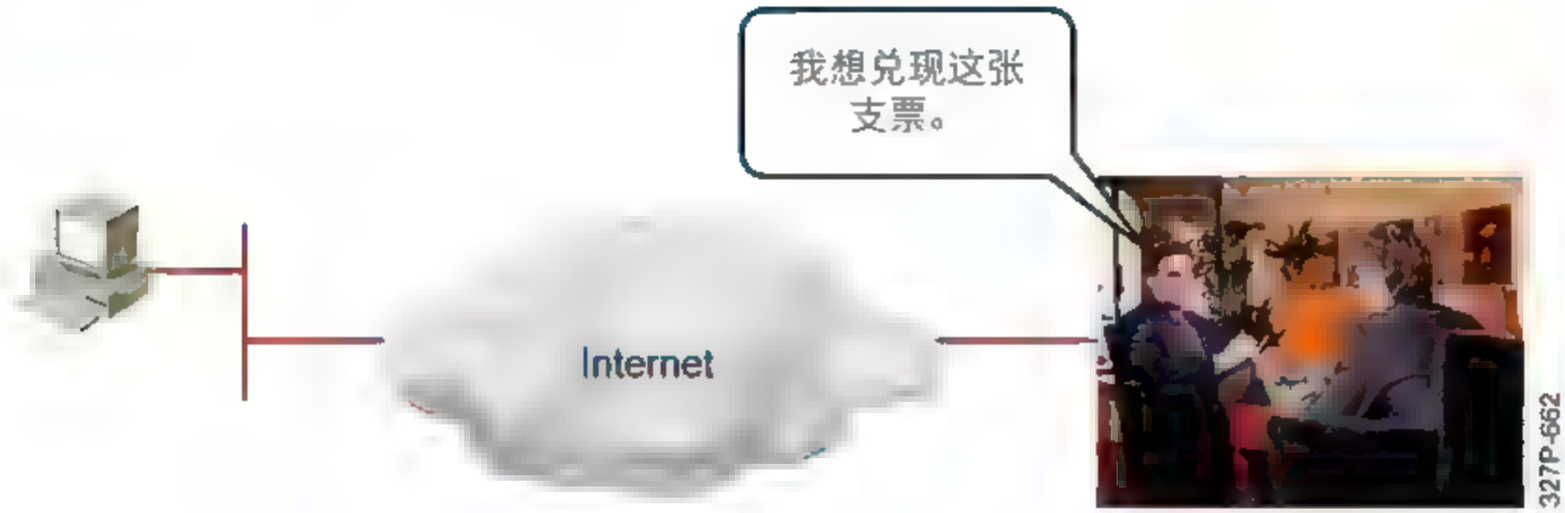
DH 密钥交换

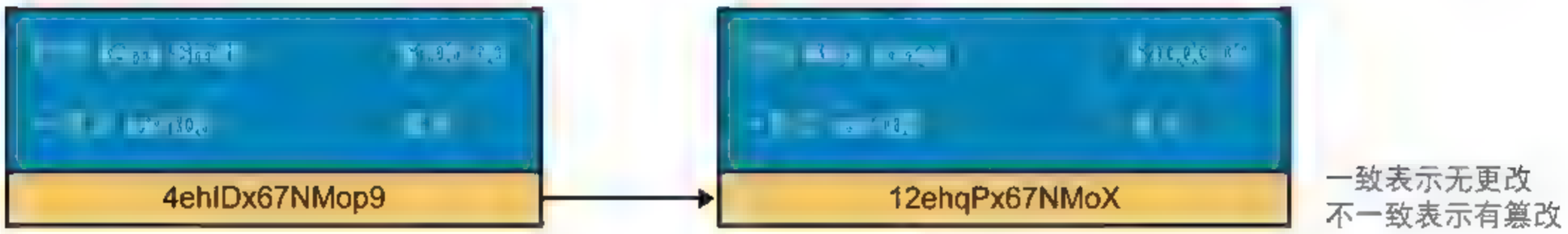


Diffie-Hellman 算法：

- DH1
- DH2
- DH5

数据完整性





哈希算法：

- HMAC-MD5
- HMAC-SHA-1

身份验证

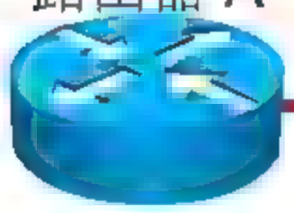
对等点身份验证方法：

- PSK
- RSA 签名

IPsec 安全协议

验证报头

路由器 A



所有数据都为明文形式

路由器 B

AH 提供以下功能：

- 身份验证
- 完整性

封装安全负载

路由器 A

数据负载

路由器 B

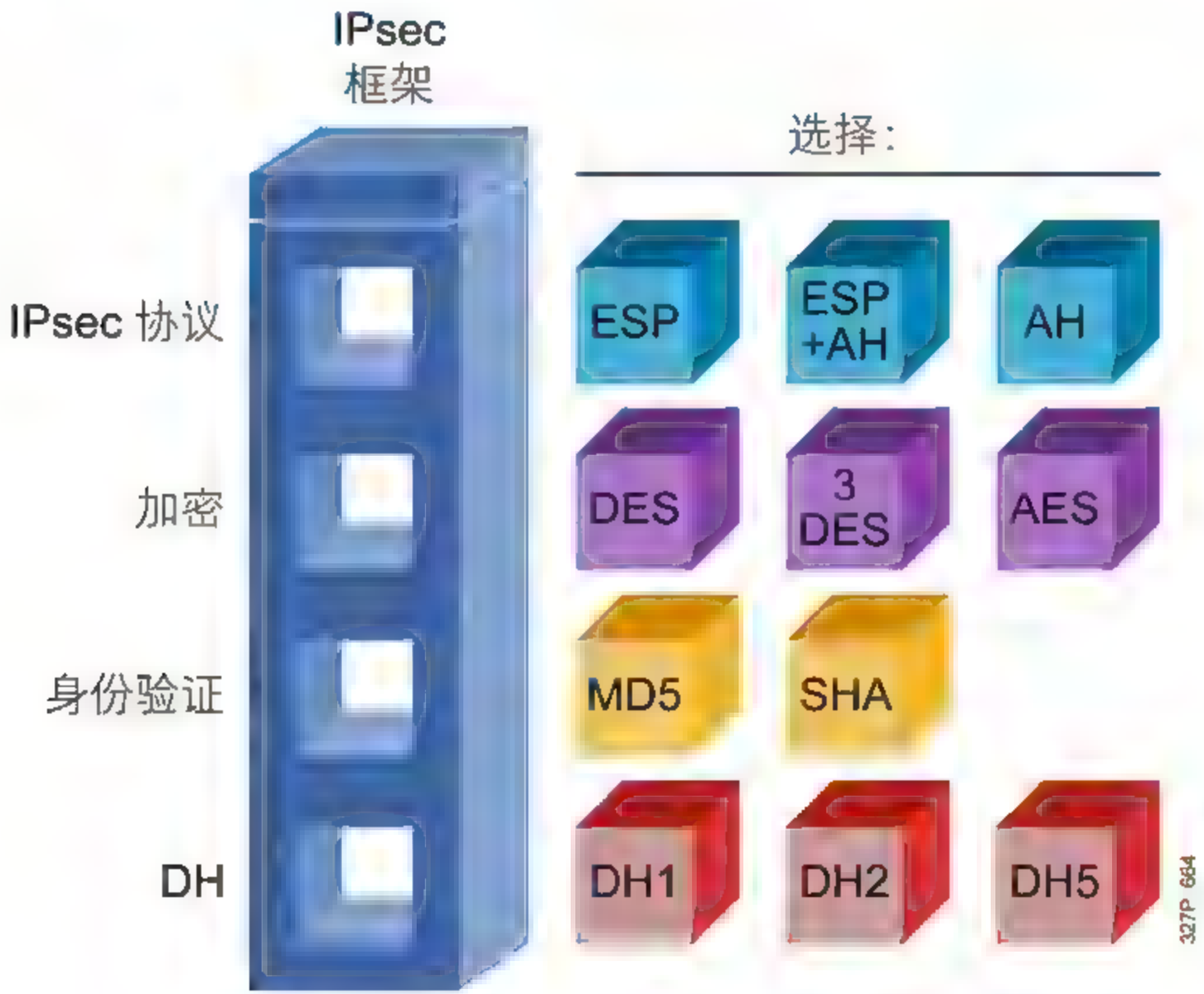
327P 072

ESP 提供以下功能：

- 加密
- 身份验证
- 完整性

© 2008 Cisco Systems, Inc. 保留所有权利。

IPsec 框架


IPsec
框架
选择:
IPsec 协议
加密
身份验证
DH
ESP
ESP +AH
AH
DES
3 DES
AES
MD5
SHA
DH1
DH2
DH5
327P 684

总结

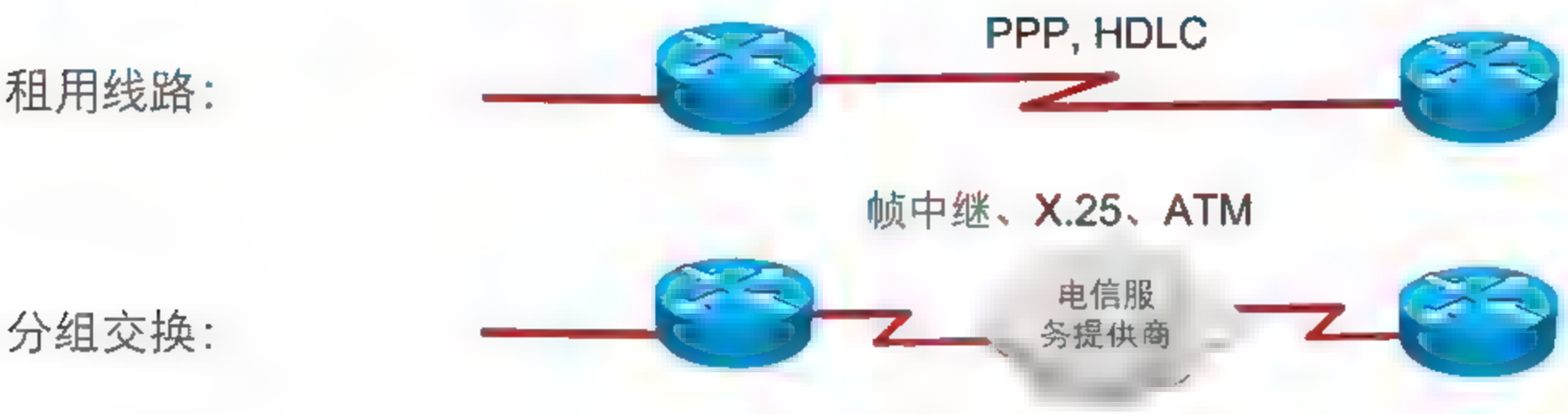
- 许多组织实施 VPN，因为 VPN 比传统 WAN 更便宜、更安全、更易于扩展。
- 站点间 VPN 对内部网和外联网对等点间的流量进行了安全保护。远程访问 VPN 对从在外旅行的电信通勤族到中央局的通信进行了安全保护。
- 可以使用各种不同的 Cisco 设备来实施 VPN：Cisco IOS 路由器、ASA 5500 系列自适应安全设备和 Cisco VPN 客户端软件。
- IPsec 是一种将多种安全协议结合在一起的框架，它向 VPN 提供数据机密性、数据完整性和身份验证。
- AH 和 ESP 是两种主要的 IPsec 框架协议。

CISCO

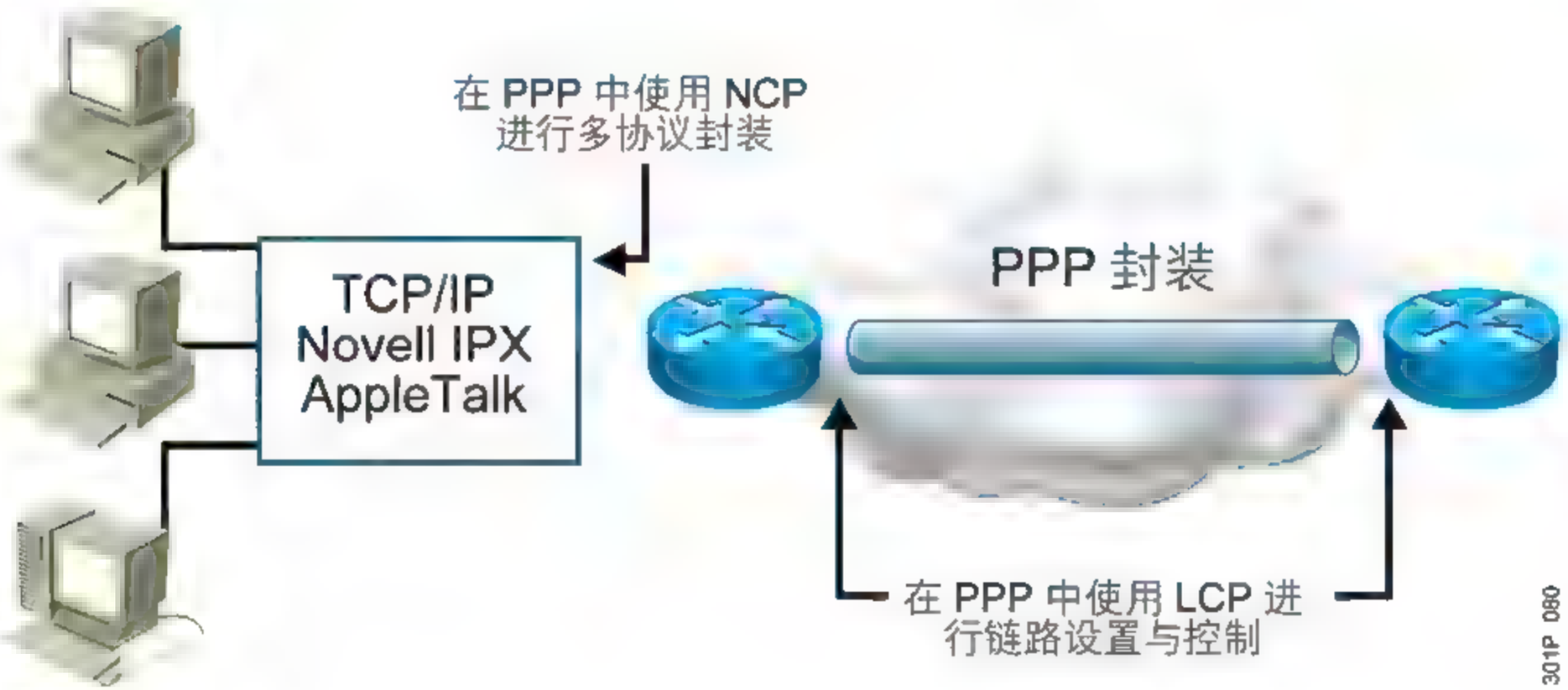
使用 PPP 建立点对点的 WAN 连接

LAN 延伸到 WAN

典型的 WAN 封装协议


租用线路:
PPP, HDLC
分组交换:
帧中继、X.25、ATM
电信服
务提供商
电路交换:
PPP, HDLC
POTS 或 ISDN
服务提供商
城域以太网:
以太网
电信服务
提供商
宽带:
PPPoE, PPPoA, 以太网
DSL、有线
提供商
Internet
服务提供商

PPP 概述



- PPP 可以使用 NCP 传输来自多种协议簇的数据包。
- PPP 使用 LCP 控制多个链路选项的设置。

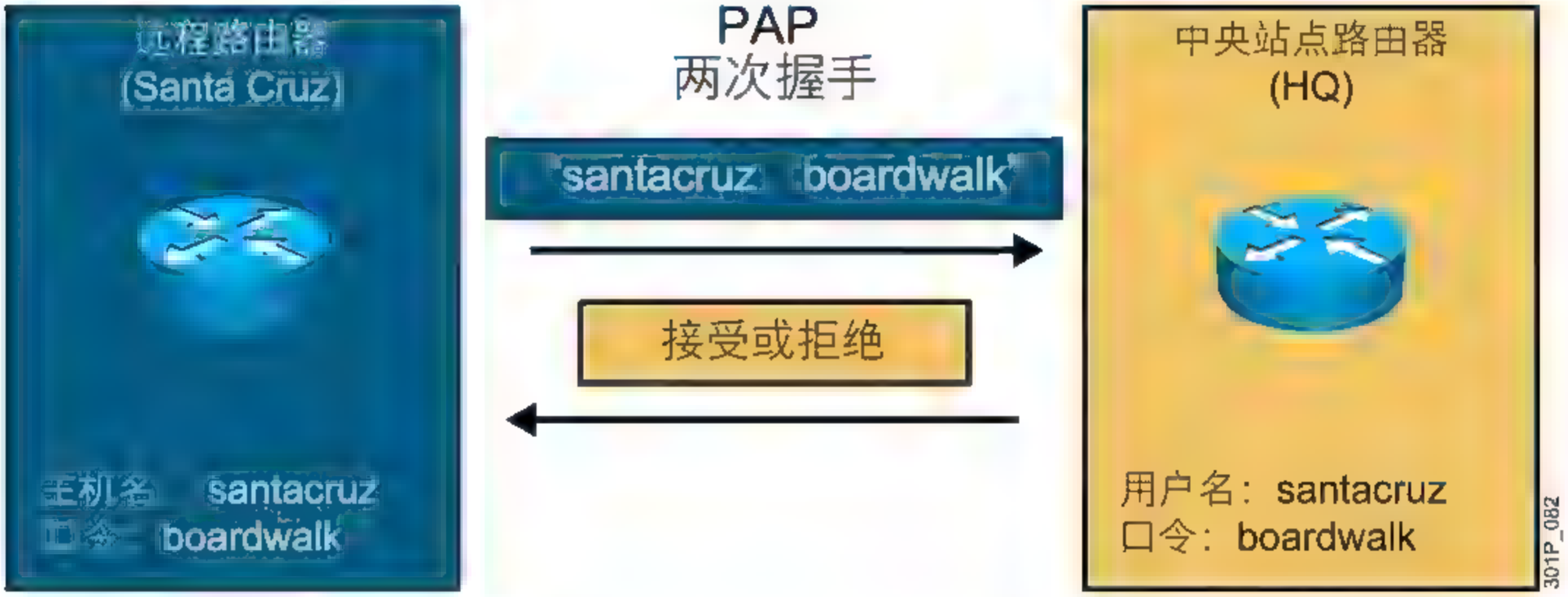
PPP 会话建立

PPP 会话建立：

1. 链路建立阶段
2. 身份验证阶段（可选）

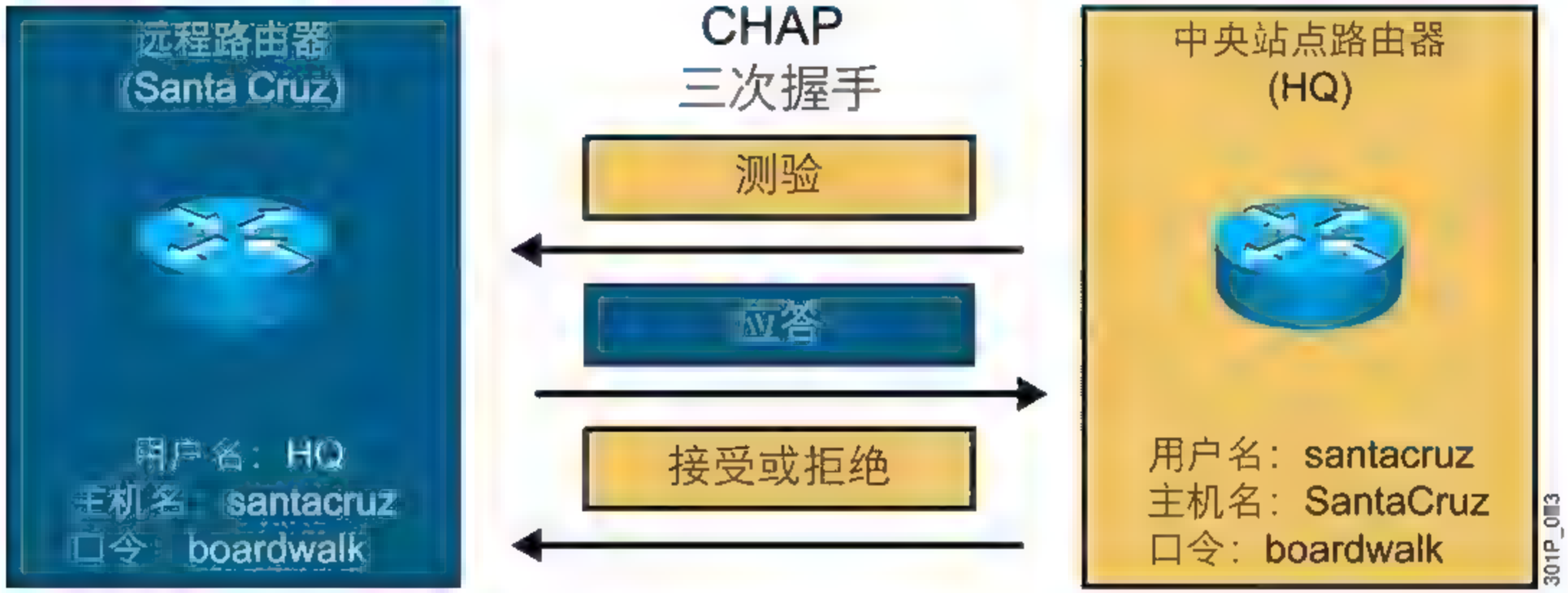
   两种 PPP 身份认证协议：PAP 和 CHAP
3. 网络层协议阶段

PPP 身份验证协议：PAP



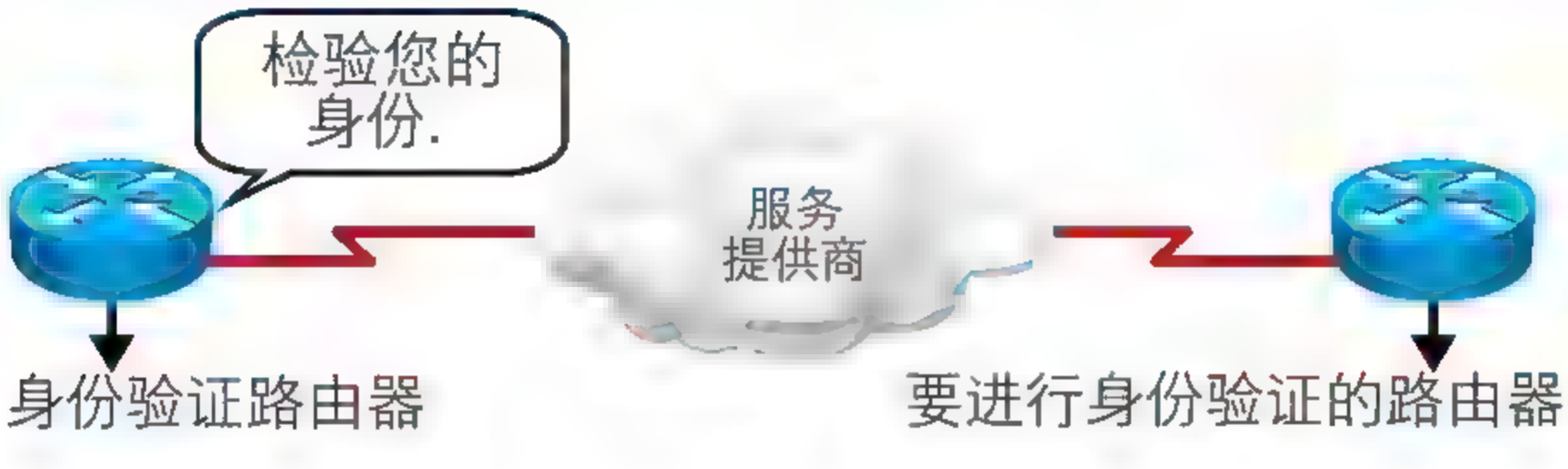
- 口令以明文发送
- 对等点控制尝试

PPP 身份验证协议：CHAP



- 这是 Santa Cruz 路由器对 HQ 路由器进行身份验证的示例。
- 通过链路发送哈希值（并非实际的口令）。
- 本地路由器或外部服务器控制身份验证尝试。

配置 PPP 和身份验证概述



启用 PPP

- ☑ PPP 封装

启用 PPP 身份验证

- ☑ 主机名
- ☑ 用户名和口令
- ☑ PPP 身份验证

启用 PPP

- ☑ PPP 封装

启用 PPP 身份验证

- ☑ 主机名
- ☑ 用户名和口令
- ☑ PPP 身份验证

配置 PPP 和身份验证

```
RouterX(config-if)# encapsulation ppp
```

- 启用 PPP 封装

```
RouterX(config)# hostname name
```

- 给路由器指定主机名

```
RouterX(config)# username name password password
```

- 标识远程路由器的用户名和口令

```
RouterX(config-if)# ppp authentication
{chap | chap pap | pap chap | pap}
```

- 启用 PAP 或 CHAP 身份验证

PPP 和 CHAP 配置示例

```
hostname RouterX
username RouterY password sameone
!
int serial 0
ip address 10.0.1.1 255.255.255.0
encapsulation ppp
ppp authentication chap
```

```
hostname RouterY
username RouterX password sameone
!
int serial 0
ip address 10.0.1.2 255.255.255.0
encapsulation ppp
ppp authentication chap
```

检验 PPP 封装配置

```
RouterX# show interface s0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:05, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     38021 packets input, 5656110 bytes, 0 no buffer
     Received 23488 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     38097 packets output, 2135697 bytes, 0 underruns
     0 output errors, 0 collisions, 6045 interface resets
     0 output buffer failures, 0 output buffers swapped out
     482 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

检验 PPP 身份验证

```
RouterX# debug ppp authentication
4d20h: %LINK-3-UPDOWN: Interface Serial0, changed state to up
4d20h: Se0 PPP: Treating connection as a dedicated line
4d20h: Se0 PPP: Phase is AUTHENTICATING, by both
4d20h: Se0 CHAP: O CHALLENGE id 2 len 28 from "left"
4d20h: Se0 CHAP: I CHALLENGE id 3 len 28 from "right"
4d20h: Se0 CHAP: O RESPONSE id 3 len 28 from "left"
4d20h: Se0 CHAP: I RESPONSE id 2 len 28 from "right"
4d20h: Se0 CHAP: O SUCCESS id 2 len 4
4d20h: Se0 CHAP: I SUCCESS id 3 len 4
4d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
```

debug ppp authentication 命令可显示成功的 CHAP 输出

检验 PPP 协商

```
RouterX# debug ppp negotiation
PPP protocol negotiation debugging is on
RouterX#
*Mar  1 00:06:36.645: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
*Mar  1 00:06:36.661: BR0:1 PPP: Treating connection as a callin
*Mar  1 00:06:36.665: BR0:1 PPP: Phase is ESTABLISHING, Passive Open
*Mar  1 00:06:36.669: BR0:1 LCP: State is Listen
*Mar  1 00:06:37.034: BR0:1 LCP: I CONFREQ [Listen] id 7 len 17
*Mar  1 00:06:37.038: BR0:1 LCP:    AuthProto PAP (0x0304C023)
*Mar  1 00:06:37.042: BR0:1 LCP:    MagicNumber 0x507A214D (0x0506507A214D)
*Mar  1 00:06:37.046: BR0:1 LCP:    Callback 0  (0x0D0300)
*Mar  1 00:06:37.054: BR0:1 LCP: O CONFREQ [Listen] id 4 len 15
*Mar  1 00:06:37.058: BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
*Mar  1 00:06:37.062: BR0:1 LCP:    MagicNumber 0x1081E7E1 (0x05061081E7E1)
*Mar  1 00:06:37.066: BR0:1 LCP: O CONFREJ [Listen] id 7 len 7
*Mar  1 00:06:37.070: BR0:1 LCP:    Callback 0  (0x0D0300)
*Mar  1 00:06:37.098: BR0:1 LCP: I CONFACK [REQsent] id 4 len 15
*Mar  1 00:06:37.102: BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
*Mar  1 00:06:37.106: BR0:1 LCP:    MagicNumber 0x1081E7E1 (0x05061081E7E1)
*Mar  1 00:06:37.114: BR0:1 LCP: I CONFREQ [ACKrcvd] id 8 len 14
*Mar  1 00:06:37.117: BR0:1 LCP:    AuthProto PAP (0x0304C023)
*Mar  1 00:06:37.121: BR0:1 LCP:    MagicNumber 0x507A214D (0x0506507A214D)
```

总结

- PPP 是适用于 WAN 的常用第 2 层协议。PPP 包括两个组件：协商连接的 LCP 和封装流量的 NCP。
- 可将 PPP 配置为使用 PAP 或 CHAP。PAP 以明文形式发送所有信息。CHAP 使用 MD5 哈希。
- 常用 PPP 验证命令包括用于检验 PPP 封装的 **show interface** 命令，以及用于检验 LCP 握手的 **debug ppp negotiation** 命令。

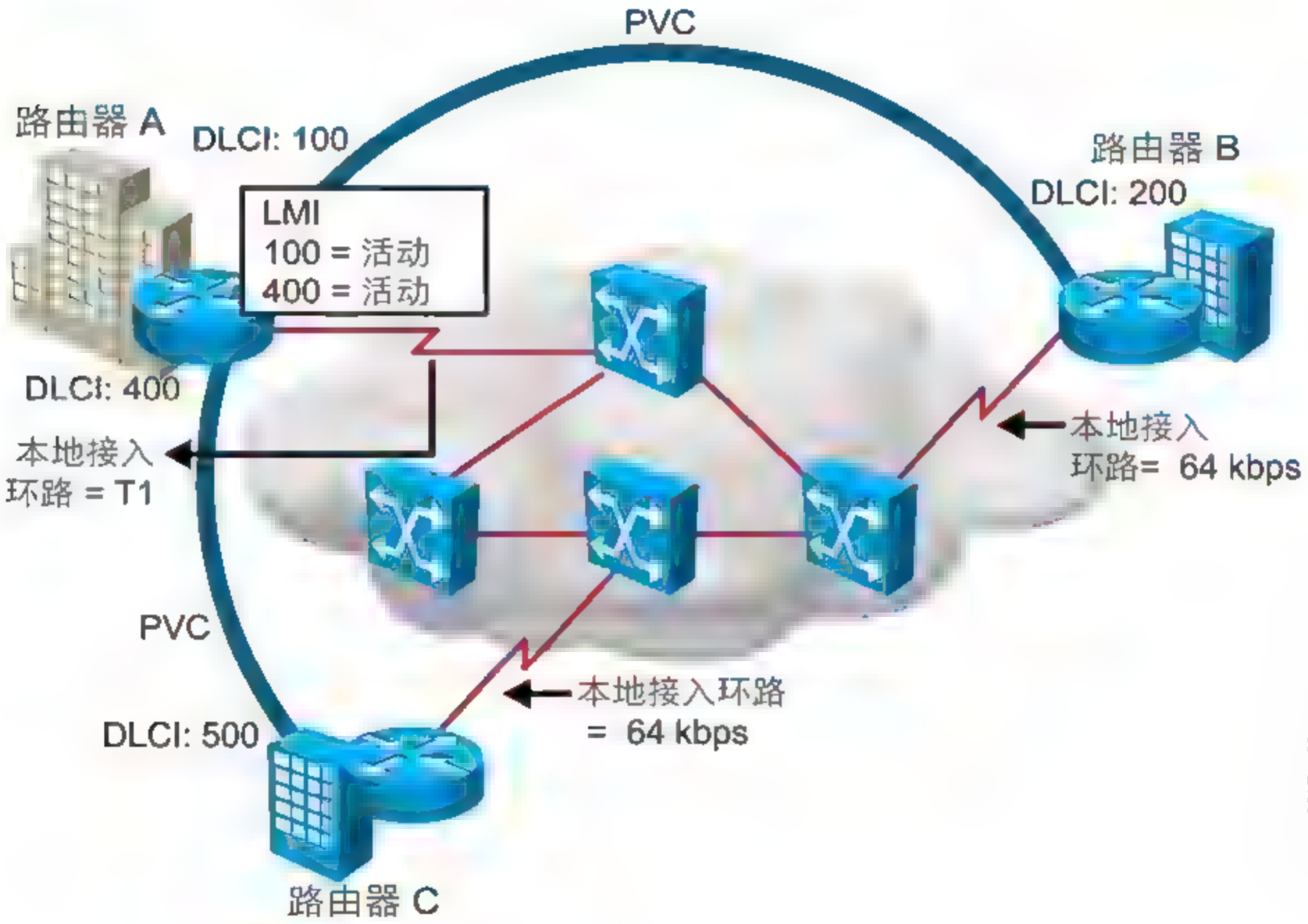
使用帧中继建立 WAN 连接

LAN 延伸到 WAN

帧中继概述

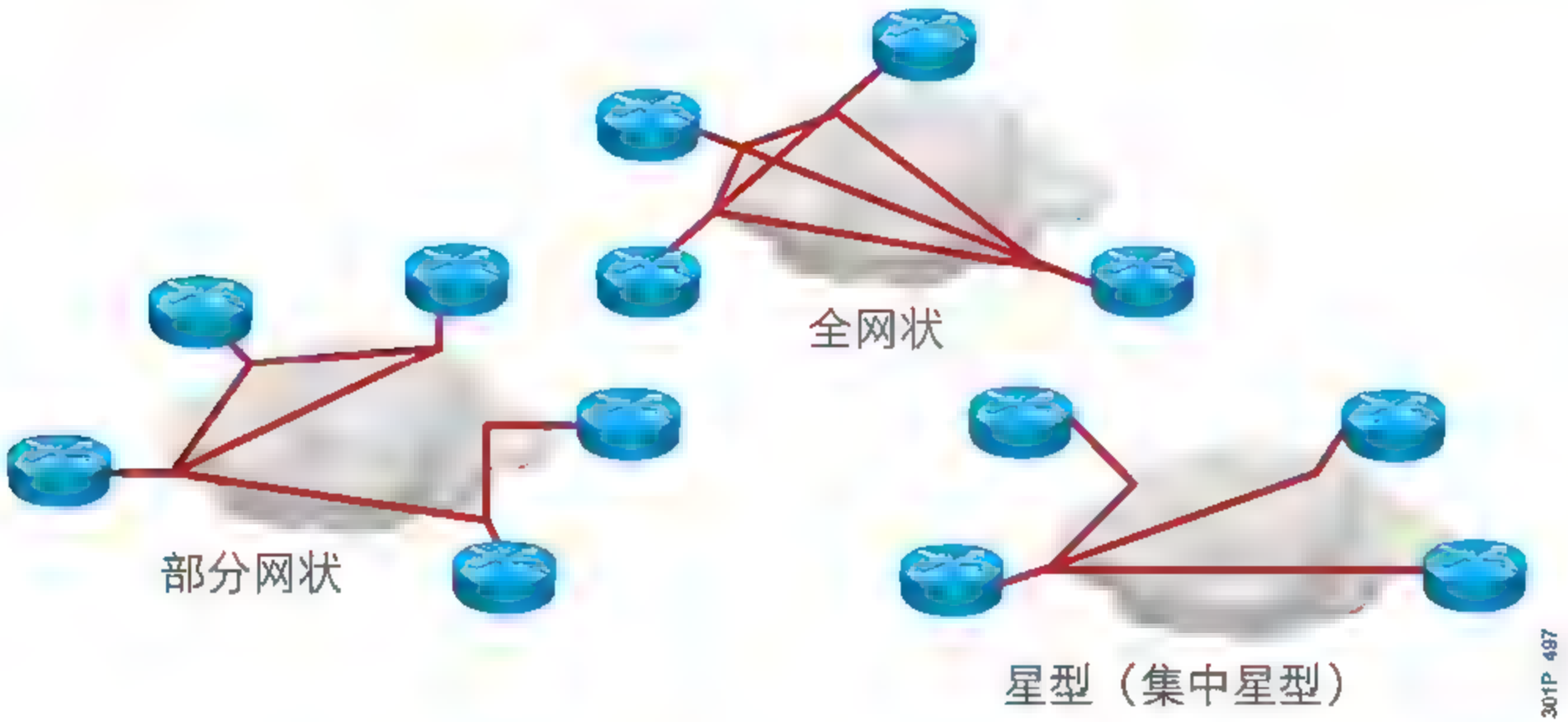
- 使用虚电路建立的连接
- 面向连接的服务

帧中继术语



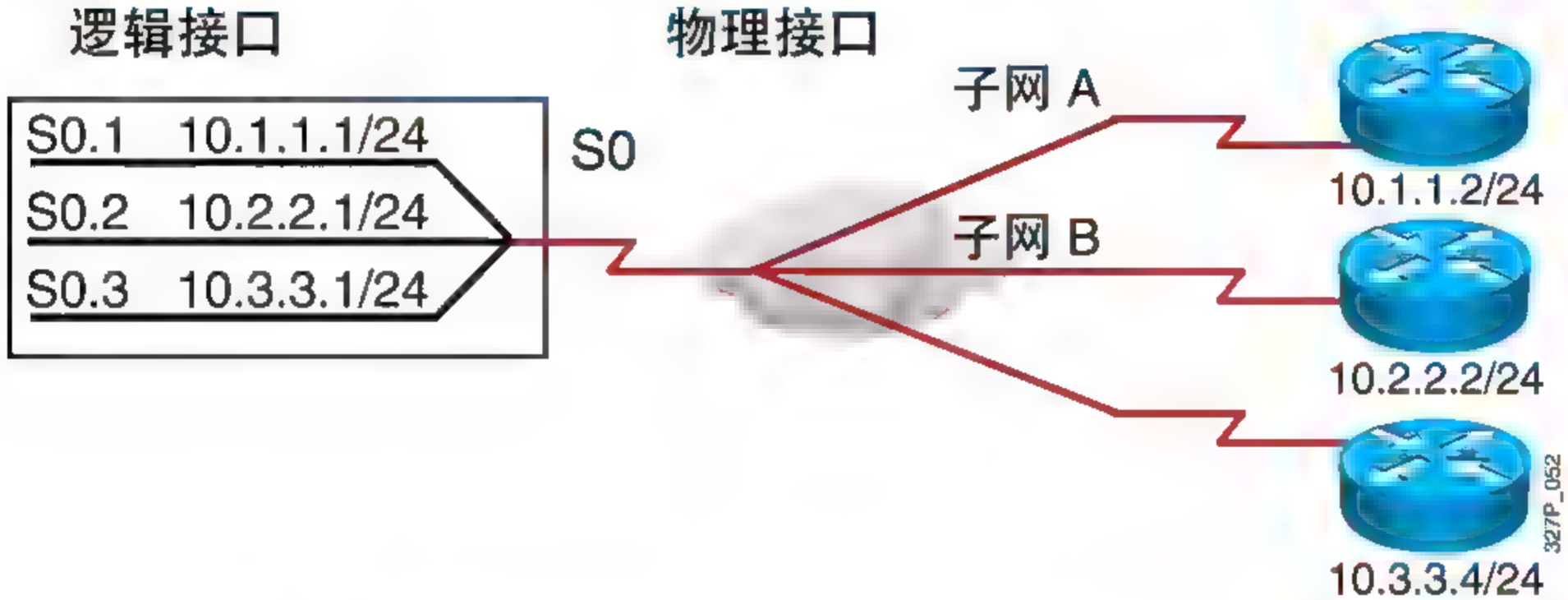
© 2008 Cisco Systems, Inc. 保留所有权利。

选择帧中继拓扑



帧中继默认值：NBMA

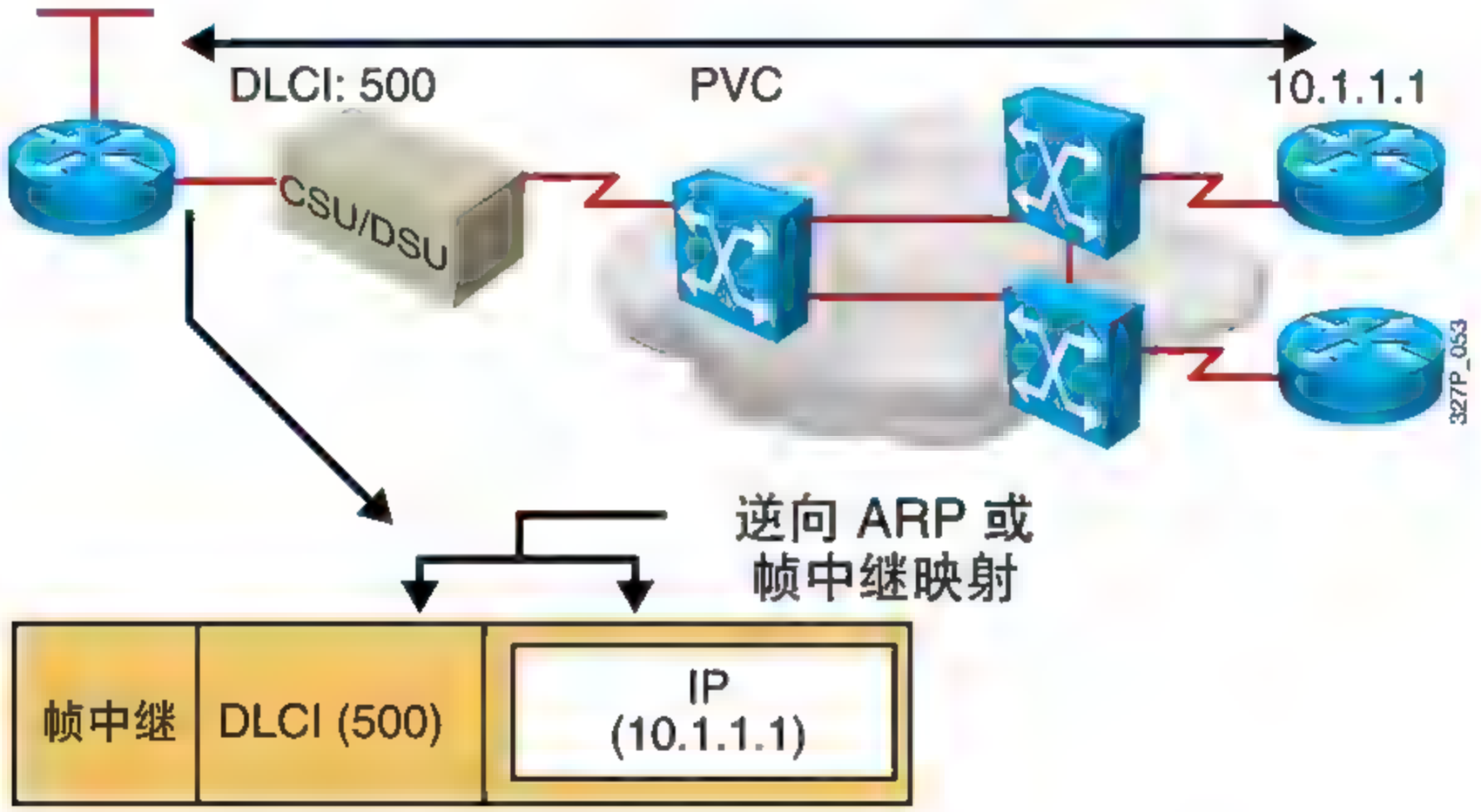
解决 NBMA 连通性问题



在 NBMA 环境中使用水平分割会出现问题。

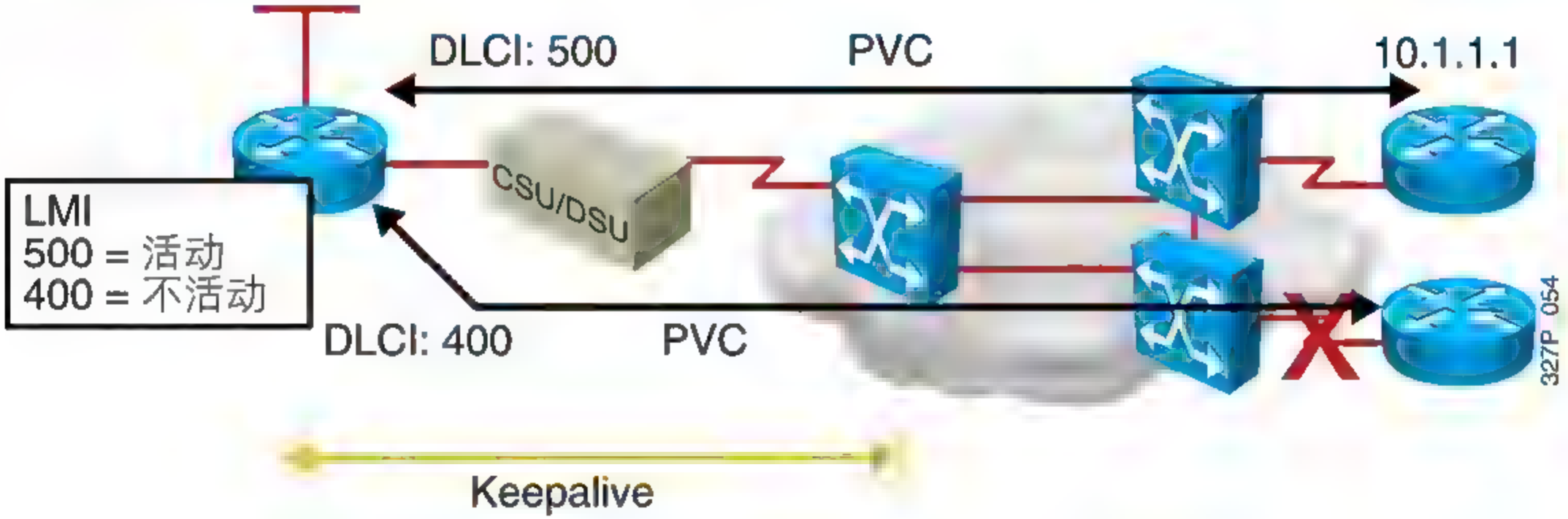
- 解决方案：子接口
- 单个物理接口模拟多个逻辑接口。

帧中继地址映射



- LMI 接收来自帧中继交换机且在本地有效的 DLCI。
- 逆向 ARP 将本地 DLCI 映射到远程路由器网络层地址。

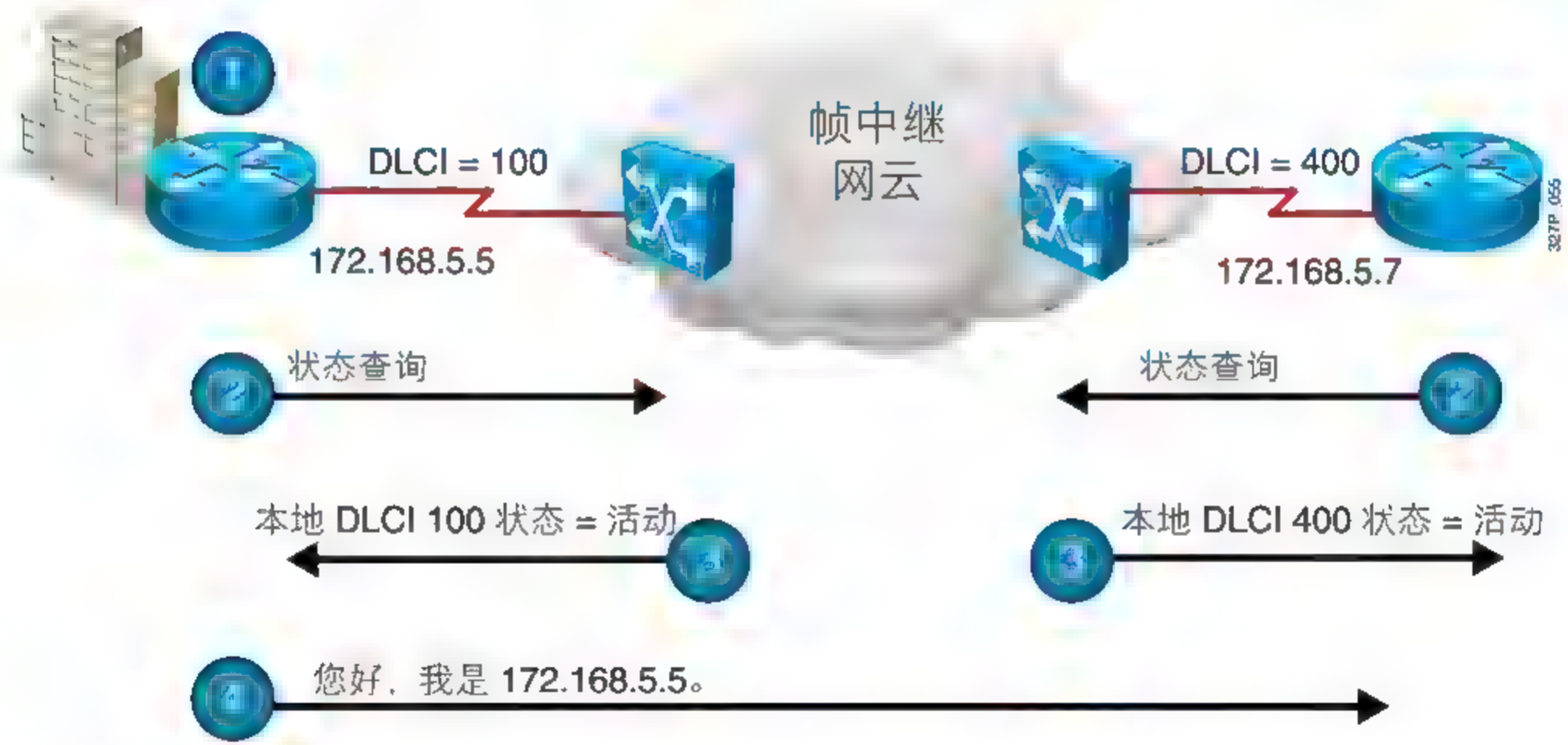
帧中继信令



Cisco 支持三种 LMI 标准：

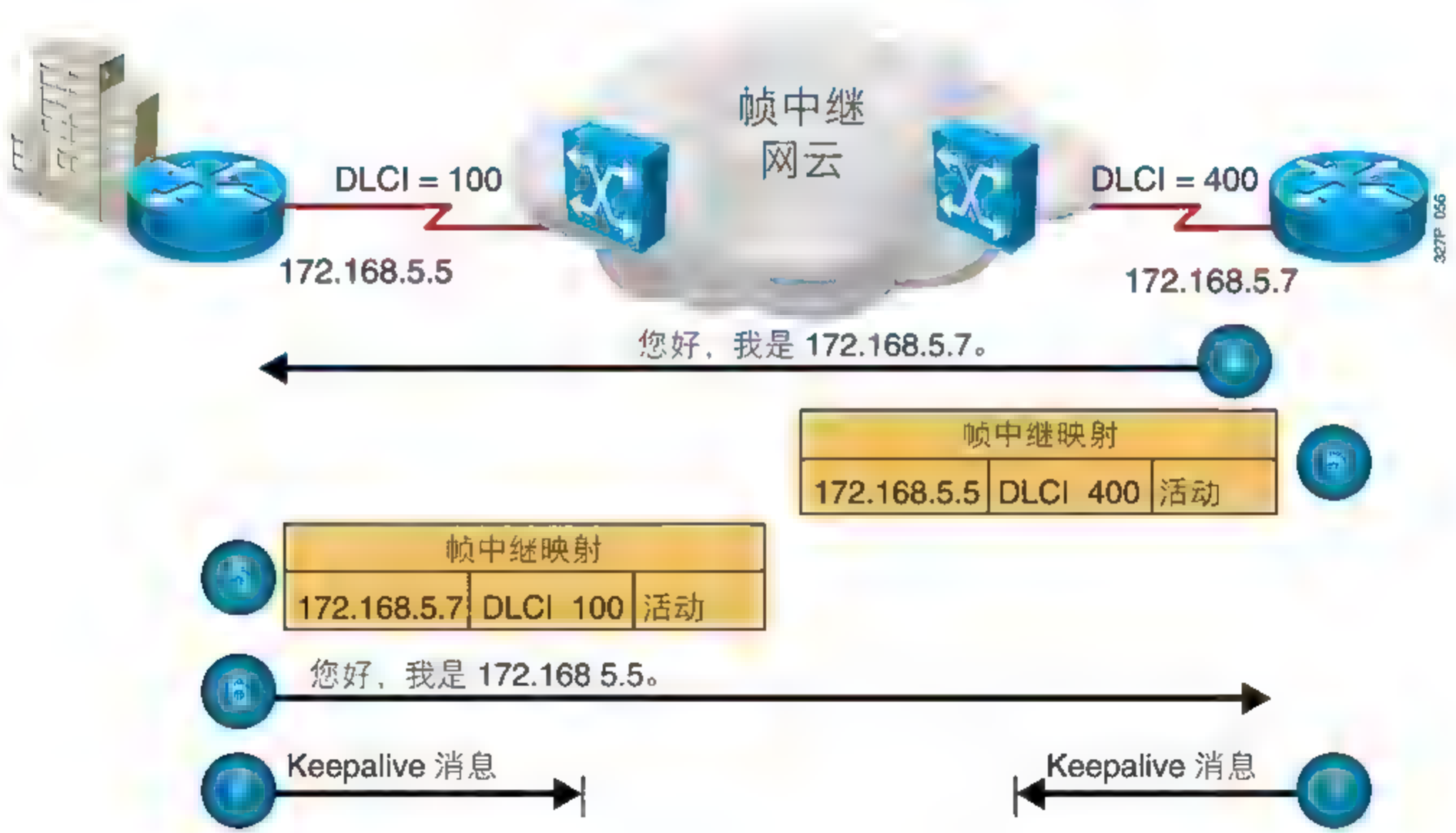
- Cisco
- ANSI T1.617 Annex D
- ITU-T Q.933 Annex A

逆向 ARP 和 LMI 的操作过程

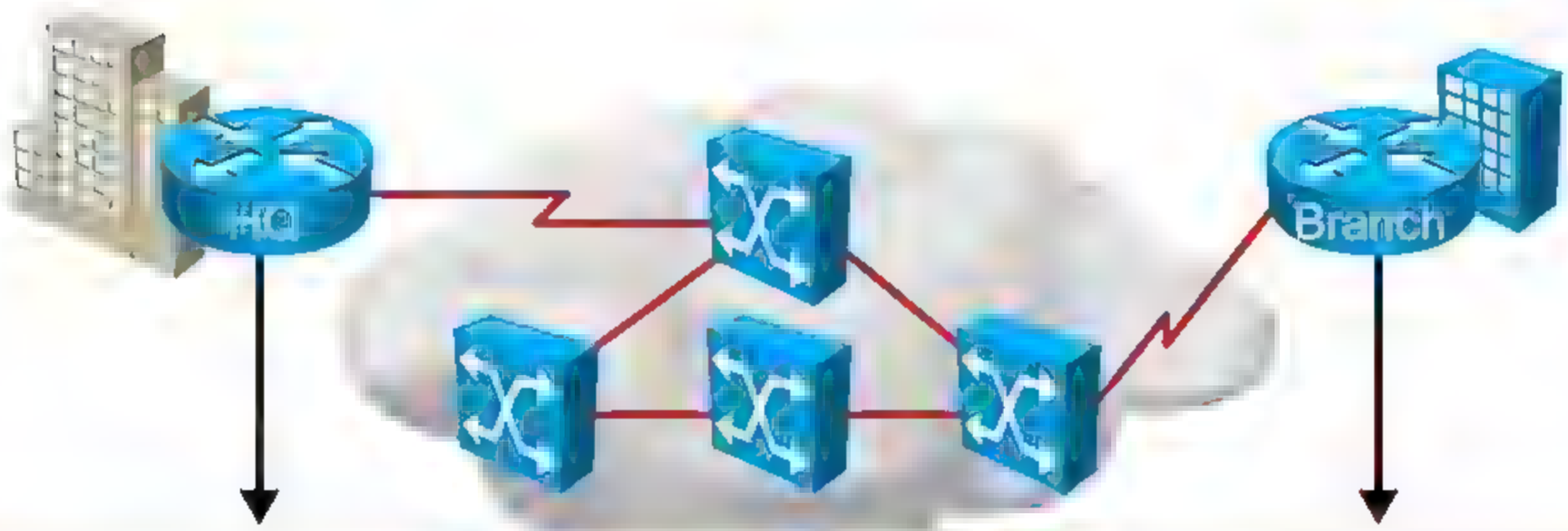


© 2008 Cisco Systems, Inc. 保留所有权利。

逆向 ARP 和 LMI 的操作过程（续）



配置基本帧中继

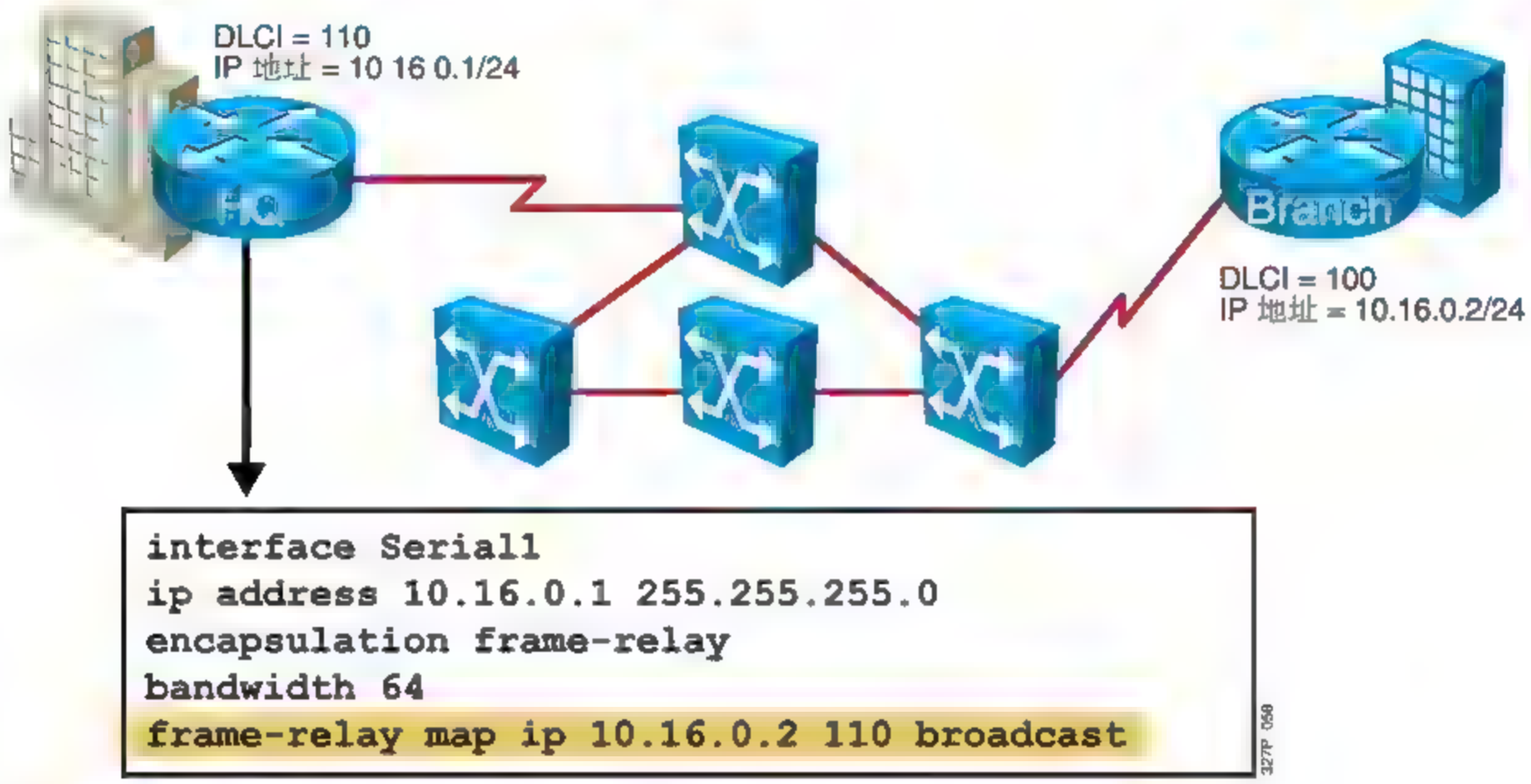



```
interface Serial1
 ip address 10.16.0.1 255.255.255.0
 encapsulation frame-relay
 bandwidth 64
```

```
interface Serial1
 ip address 10.16.0.2 255.255.255.0
 encapsulation frame-relay
 bandwidth 64
```

327P 057

配置静态帧中继映射



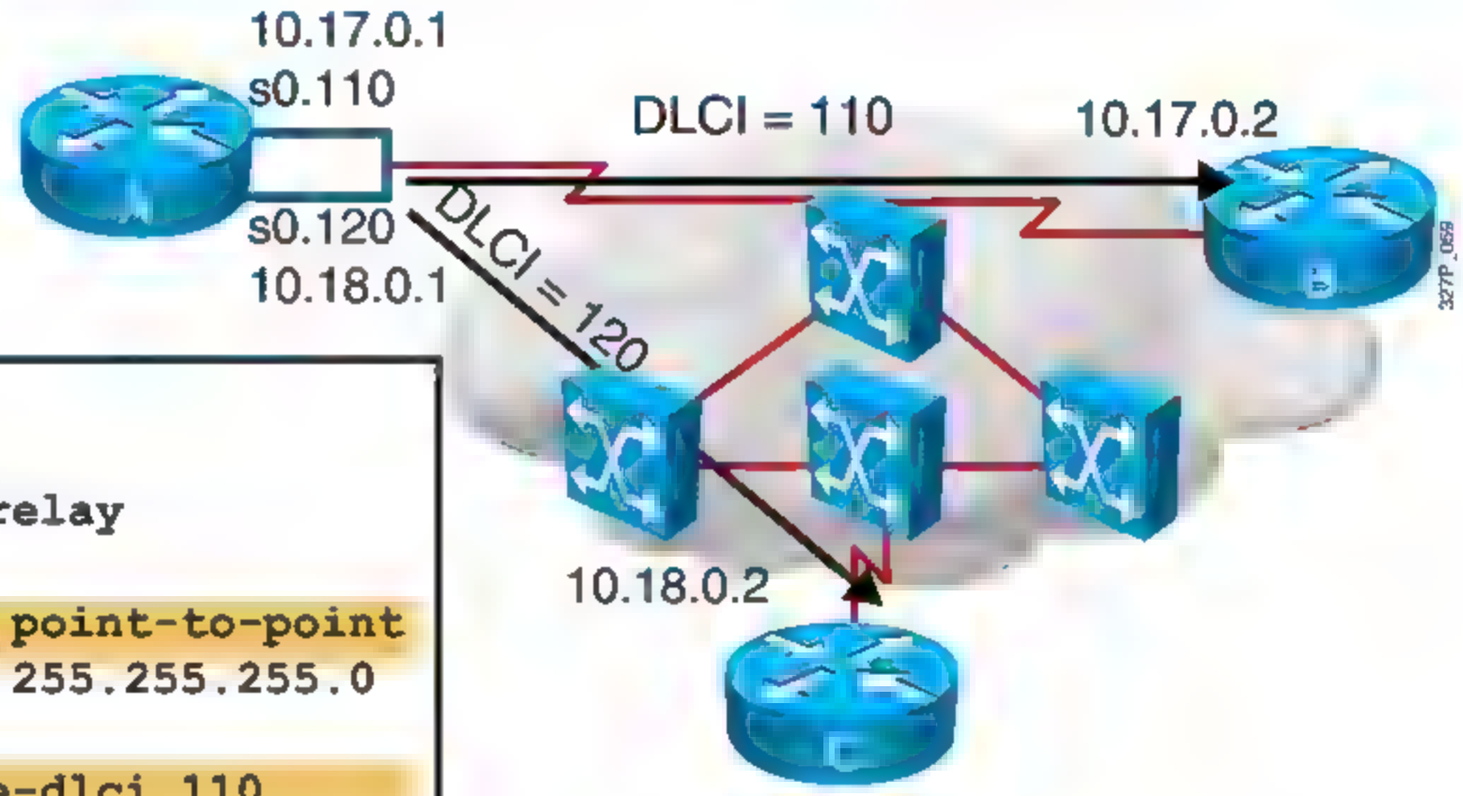
在以下情况中配置静态帧中继映射：

- 帧中继对等点不支持逆向 ARP
- 需要控制 PVC 上的广播流量
- 需要在 PVC 上拥有不同的帧中继封装

配置帧中继子接口

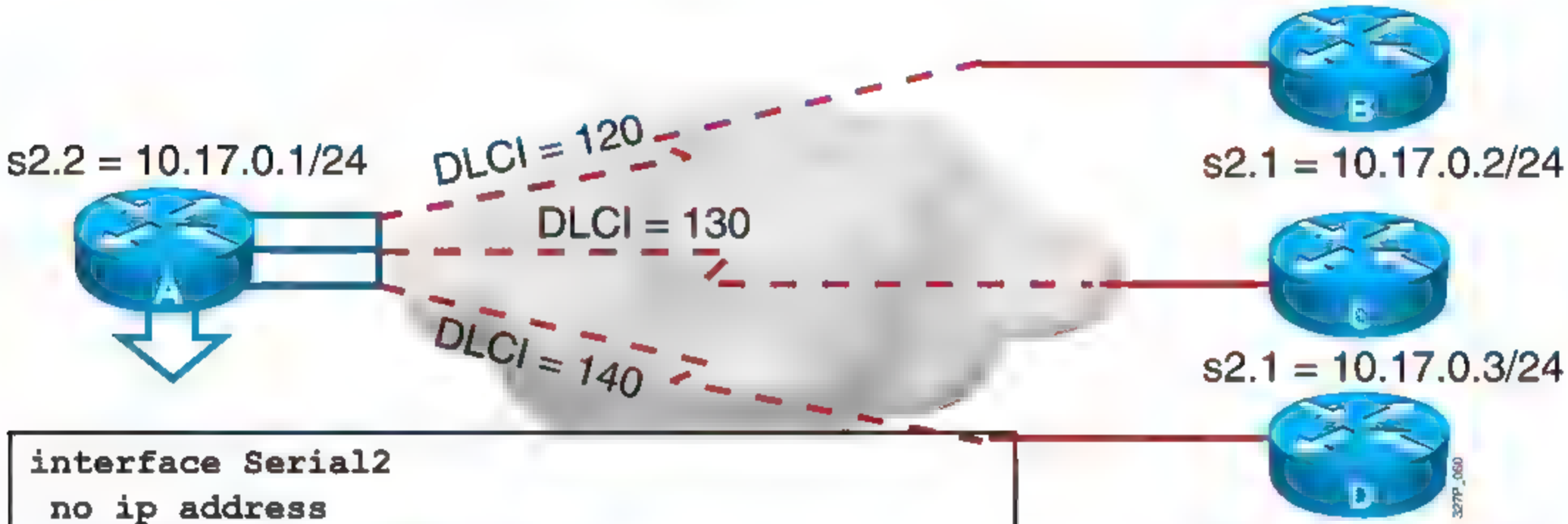
- 点对点
  - 此类子接口的作用相当于租用线路。
  - 每个点对点子接口需要拥有自己的子网。
  - 点对点子接口适用于集中星型拓扑。
- 多点
  - 此类子接口的作用相当于 NBMA 网络，因此它们不解决水平分割问题。
  - 多点子接口可节省地址空间，因为它使用单一子网。
  - 多点子接口适用于偏网状拓扑和全网状拓扑。

配置帧中继点对点子接口




```
interface Serial0
 no ip address
 encapsulation frame-relay
!
interface Serial0.110 point-to-point
 ip address 10.17.0.1 255.255.255.0
 bandwidth 64
 frame-relay interface-dlci 110
!
interface Serial0.120 point-to-point
 ip address 10.18.0.1 255.255.255.0
 bandwidth 64
 frame-relay interface-dlci 120
!
```

配置帧中继多点子接口




```
interface Serial2
 no ip address
 encapsulation frame-relay
!
interface Serial2.2 multipoint
 ip address 10.17.0.1 255.255.255.0
 bandwidth 64
 frame-relay map ip 10.17.0.2 120 broadcast
 frame-relay map ip 10.17.0.3 130 broadcast
 frame-relay map ip 10.17.0.4 140 broadcast
```

检验帧中继运行

```
RouterX# show interfaces type number
```

- 显示有关帧中继 DLCI 和 LMI 的信息

```
RouterX# show interfaces s0
Serial0 is up, line protocol is up
Hardware is HD64570
Internet address is 10.140.1.2/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation FRAME-RELAY, loopback not set, keepalive set (10 sec)
LMI enq sent  19, LMI stat recvd 20, LMI upd recvd 0, DTE LMI up
LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
LMI DLCI 1023  LMI type is CISCO  frame relay DTE
FR SVC disabled, LAPF state down
Broadcast queue 0/64, broadcasts sent/dropped 8/0, interface broadcasts 5
Last input 00:00:02, output 00:00:02, output hang never
Last clearing of "show interface" counters never
Queueing strategy:fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
<省略部分输出>
```

检验帧中继运行（续）

```
RouterX# show frame-relay lmi [type number]
```

- 显示 LMI 统计信息

```
RouterX# show frame-relay lmi

LMI Statistics for interface Serial0 (Frame Relay DTE) LMI TYPE = CISCO
Invalid Unnumbered info 0 Invalid Prot Disc 0
Invalid dummy Call Ref 0 Invalid Msg Type 0
Invalid Status Message 0 Invalid Lock Shift 0
Invalid Information ID 0 Invalid Report IE Len 0
Invalid Report Request 0 Invalid Keep IE Len 0
Num Status Enq.Sent 113100 Num Status msgs Rcvd 113100
Num Update Status Rcvd 0 Num Status Timeouts 0
```

检验帧中继运行（续）

```
RouterX# debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
RouterX#
1w2d:Serial0(out):StEnq, myseq 140, yourseen 139, DTE up
1w2d:datagramstart = 0xE008EC, datagramsize = 13
1w2d:FR encap = 0xFCF10309
1w2d:00 75 01 01 01 03 02 8C 8B
1w2d:
1w2d:Serial0(in):Status, myseq 140
1w2d:RT IE 1, length 1, type 1
1w2d:KA IE 3, length 2, yourseq 140, myseq 140
1w2d:Serial0(out):StEnq, myseq 141, yourseen 140, DTE up
1w2d:datagramstart = 0xE008EC, datagramsize = 13
1w2d:FR encap = 0xFCF10309
1w2d:00 75 01 01 01 03 02 8D 8C
1w2d:
1w2d:Serial0(in):Status, myseq 142
1w2d:RT IE 1, length 1, type 0
1w2d:KA IE 3, length 2, yourseq 142, myseq 142
1w2d:PVC IE 0x7 , length 0x6 , dlci 100, status 0x2 , bw 0
```

- 显示 LMI 调试信息

检验帧中继运行（续）

```
RouterX# show frame-relay pvc [type number [dlci]]
```

- 显示 PVC 统计信息

```
RouterX# show frame-relay pvc 100

PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

 input pkts 28                  output pkts 10                 in bytes 8398
 out bytes 1198                 dropped pkts 0                 in FECN pkts 0
 in BECN pkts 0                 out FECN pkts 0                out BECN pkts 0
 in DE pkts 0                   out DE pkts 0
 out bcast pkts 10              out bcast bytes 1198
 pvc create time 00:03:46, last time pvc status changed 00:03:47
```

检验帧中继运行（续）

```
RouterX# show frame-relay map
```

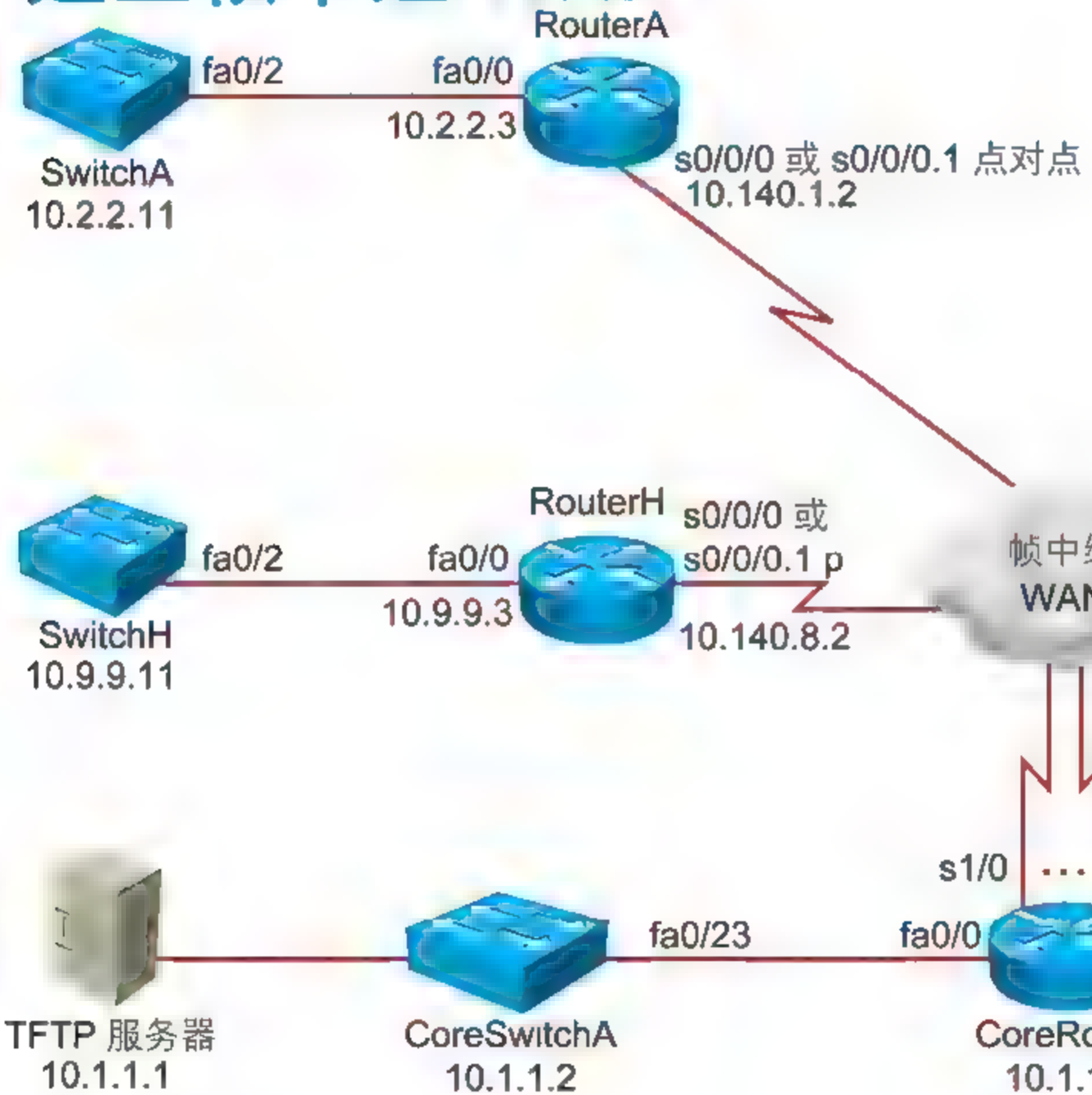
- 显示当前的帧中继映射条目

```
RouterX# clear frame-relay-inarp
```

- 动态清除使用逆向 ARP 动态创建的帧中继映射

```
RouterX# show frame-relay map
Serial0 (up):ip 10.140.1.1 dlci 100(0x64,0x1840), dynamic,
broadcast,, status defined, active
RouterX# clear frame-relay-inarp
RouterX# show frame map
RouterX#
```

可视目标 8-1：建立帧中继 WAN



工作组	路由器 s0/0/0
A	10.140.1.2
B	10.140.2.2
C	10.140.3.2
D	10.140.4.2
E	10.140.5.2
F	10.140.6.2
G	10.140.7.2
H	10.140.8.2

3279_859

© 2008 Cisco Systems, Inc. 保留所有权利。

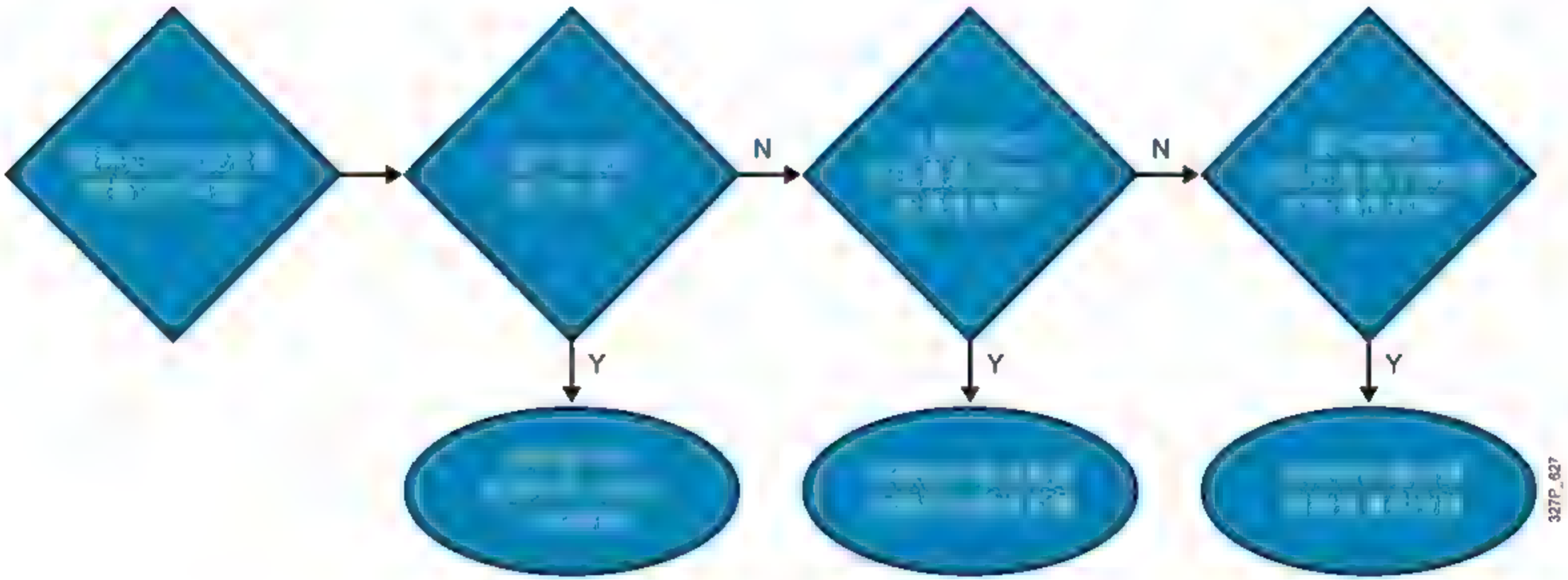
总结

- 帧中继 PVC 由 DLCI 标识，PVC 的状态通过 LMI 协议报告。
- 帧中继点对点子接口要求每条 PVC 都具有独立的子网，而多点子接口则与帧中继对等点共享单个子网。
- 要显示与帧中继提供者的连通性，可使用 **show frame-relay lmi** 命令。要显示与帧中继对等点的连通性，可使用 **show frame-relay pvc** 命令和 **show frame-relay map** 命令。

帧中继 WAN 故障排除

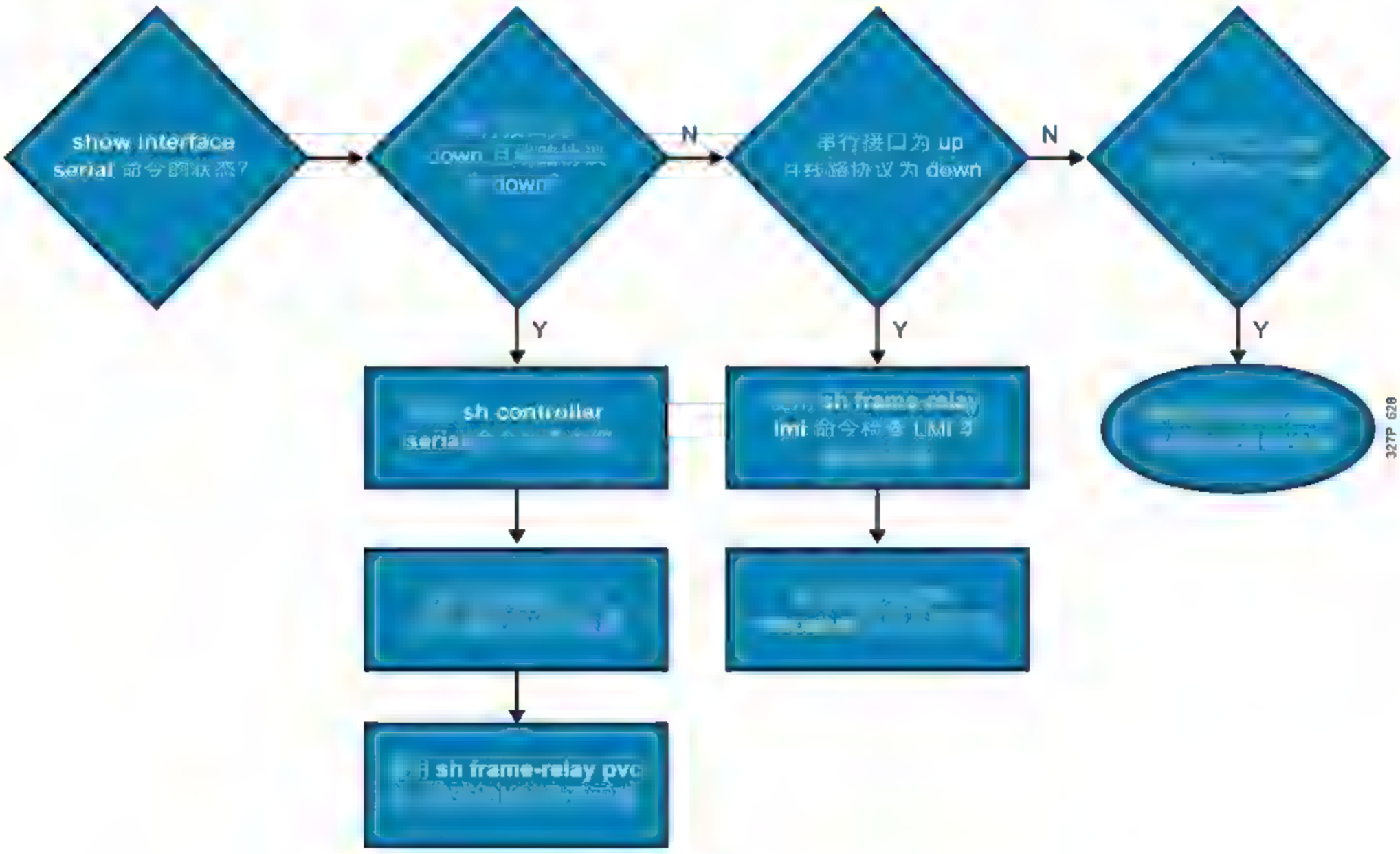
LAN 延伸到 WAN

帧中继故障排除的步骤



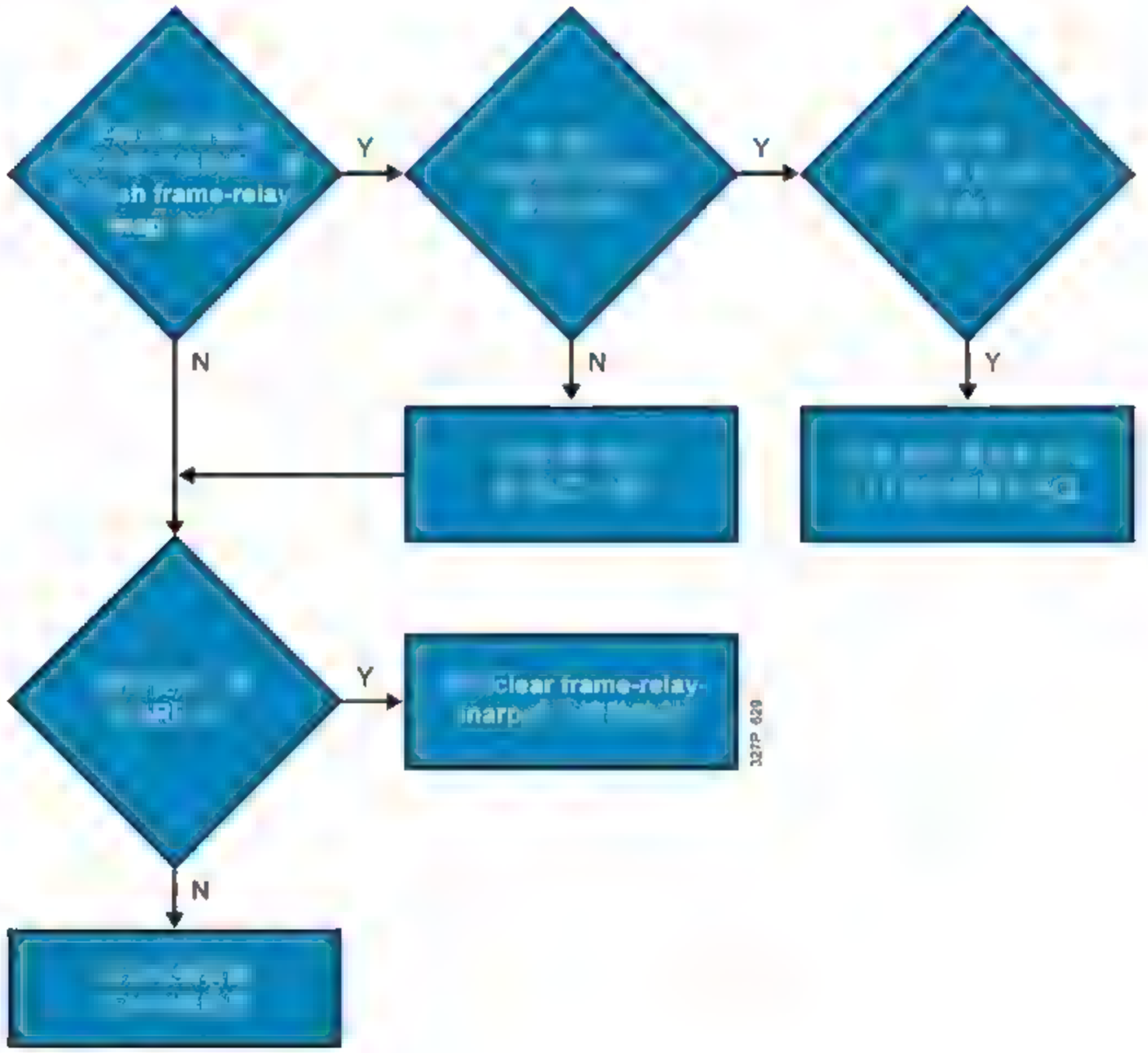
© 2008 Cisco Systems, Inc. 保留所有权利。

排除断开的帧中继链路的故障



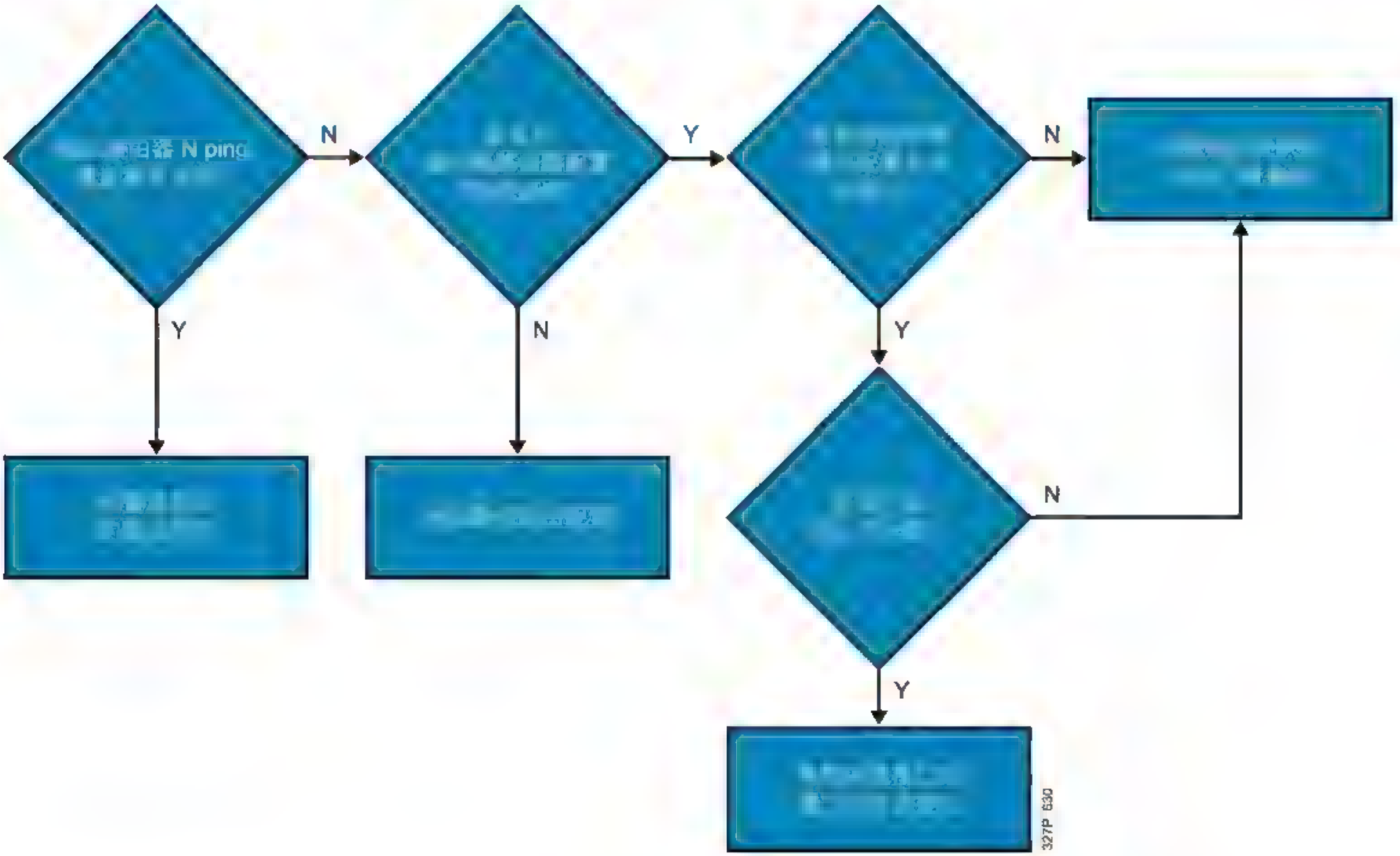
© 2008 Cisco Systems, Inc. 保留所有权利。

排除帧中继远程路由器的连通性故障



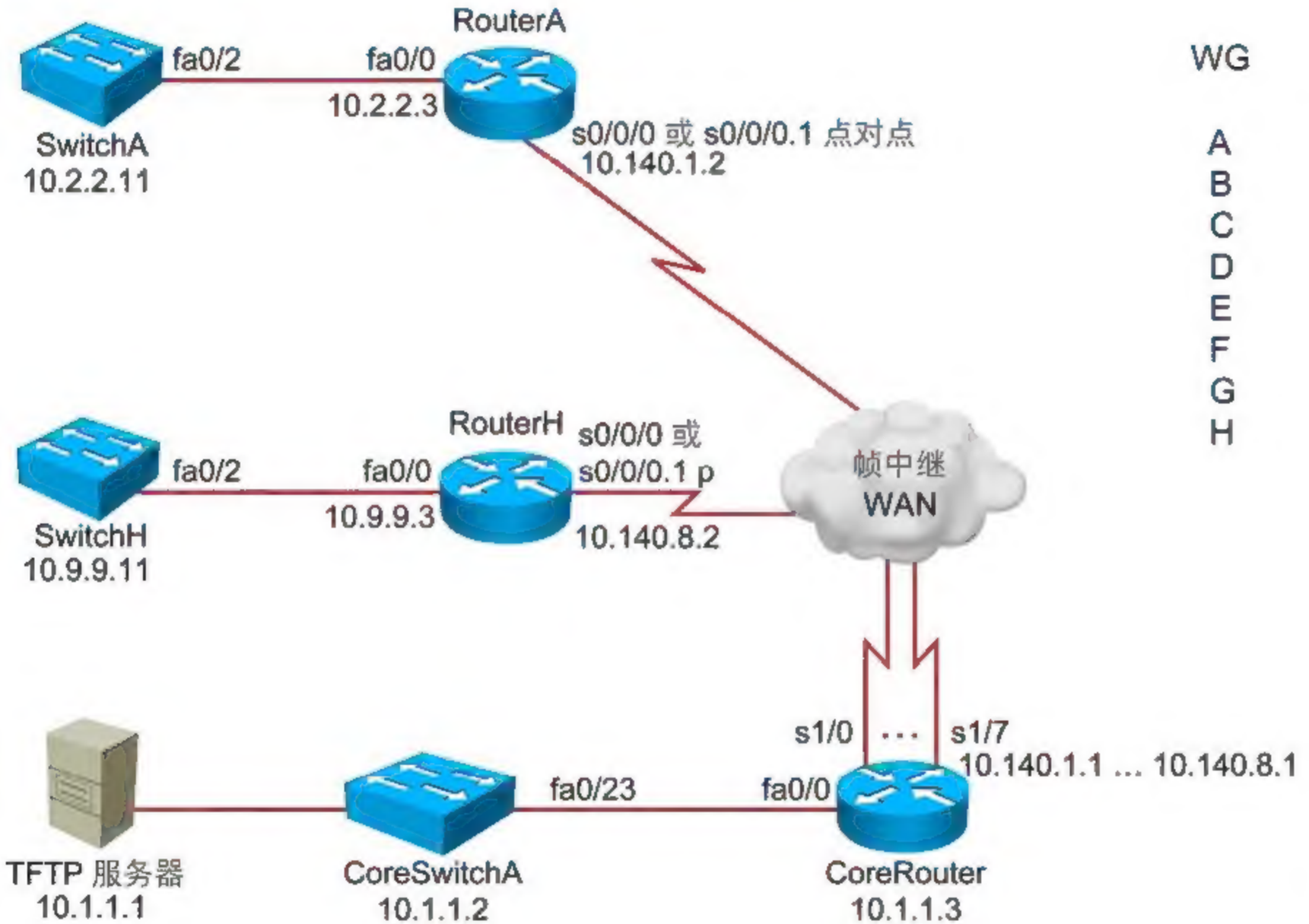
© 2008 Cisco Systems, Inc. 保留所有权利。

排除帧中继端到端连通性的故障



© 2008 Cisco Systems, Inc. 保留所有权利。

可视目标 8-2：帧中继 WAN 故障排除



WG	路由器 s0/0/0
A	10.140.1.2
B	10.140.2.2
C	10.140.3.2
D	10.140.4.2
E	10.140.5.2
F	10.140.6.2
G	10.140.7.2
H	10.140.8.2

© 2008 Cisco Systems, Inc. 保留所有权利。

总结

- 排除帧中继故障有三个方面：排除链路故障，排除从一个路由器到另一个路由器的映射故障，以及排除跨越帧中继网络的路由故障。
- 使用 **show interface serial** 命令和 **show frame-relay lmi** 命令检验第 1 层和第 2 层链路故障。使用 **show frame-relay map** 命令和 **show frame-relay pvc** 命令测试路由器间的连通性。

© 2008 Cisco Systems, Inc. 保留所有权利。

© 2008 Cisco Systems, Inc. 保留所有权利。

单元总结

- 站点间 VPN 对内部网和外联网对等点间的流量进行安全保护。远程访问 VPN 对从电信通勤族到中央局的通信进行安全保护。
- 异步和同步点对点链路上均可以配置 PPP。PPP 既支持 PAP 身份验证，也支持 CHAP 身份验证。
- 帧中继接口可以是点对点接口或多点接口。
- 要排除帧中继的连接故障，可使用 **show frame relay lmi** 命令、**show frame relay pvc** 命令和 **show frame relay map** 命令。

© 2008 Cisco Systems, Inc. 保留所有权利。